



# NATIONAL SECURITY AGENCY INFORMATION ASSURANCE DIRECTORATE

# Commercial Solutions for Classified (CSfC) Campus IEEE 802.11 Wireless Local Area Network (WLAN) Capability Package

Version 1.1 March 04, 2014

# **CHANGE HISTORY**

| Title   | Version | Date                 | Change Description  |
|---|---------|----------------------|---|
| Commercial Solutions for Classified (CSfC) Campus IEEE 802.11 Wireless Local Area Network (WLAN) Capability Package | 0.9     | December 14,<br>2012 | Initial release of CSfC Campus IEEE<br>802.11 Wireless Local Area Network<br>(WLAN) guidance.   |
| Commercial Solutions for Classified (CSfC) Campus IEEE 802.11 Wireless Local Area Network (WLAN) Capability Package | 1.0     | August 20,<br>2013   | <ul> <li>Official release of CSfC Campus WLAN guidance.</li> <li>Revised content to be consistent with VPN CP version 2.0.</li> <li>Removed compound requirements for improved testability.</li> <li>Merged sections to reduce duplicate requirements.</li> </ul> |
| Commercial Solutions for Classified (CSfC) Campus IEEE 802.11 Wireless Local Area Network (WLAN) Capability Package | 1.1     | March 4, 2014        | <ul> <li>Corrected minor errors</li> <li>Removed redundant requirements</li> <li>Added Solution testing section</li> <li>Added Appendix F to state summary of changes in requirements between the versions</li> </ul>   |

# **TABLE OF CONTENTS**

| 1 | INTI | RODUCTION                                     | 2  |
|---|------|---|----|
| 2 | PUR  | POSE OF THIS DOCUMENT                         | 2  |
| 3 | USE  | OF THIS DOCUMENT                              | 2  |
| 4 | DES  | CRIPTION OF CAMPUS IEEE 802.11 WLAN SOLUTION  | 3  |
|   | 4.1  | Networks                                      |    |
|   |      | 4.1.1 Red Network                             |    |
|   |      | 4.1.2 Gray Network                            | 5  |
|   |      | 4.1.3 Black Network                           | 5  |
|   | 4.2  | CAMPUS IEEE 802.11 WLAN SOLUTION ARCHITECTURE | 5  |
|   | 4.3  | Interactions with Enterprise Services         | 6  |
| 5 | END  | USER DEVICE                                   | 7  |
|   | 5.1  | END USER DEVICE (EUD) PROTECTION              | 7  |
|   | 5.2  | WLAN CLIENT                                   | 8  |
|   | 5.3  | VPN CLIENT                                    | 8  |
|   | 5.4  | CLIENT APPLICATIONS                           | 9  |
|   | 5.5  | GAP ANALYSIS                                  | 9  |
| 6 | CAN  | 1PUS WLAN ARCHITECTURE COMPONENTS             | 10 |
|   | 6.1  | Wireless System                               | 10 |
|   | 6.2  | WIRELESS INTRUSION DETECTION SYSTEM           | 11 |
|   | 6.3  | WLAN AUTHENTICATION SERVER                    | 11 |
|   | 6.4  | Administration Workstations                   | 11 |
|   | 6.5  | CERTIFICATE AUTHORITY                         | 12 |
|   | 6.6  | VPN GATEWAY                                   | 13 |
|   | 6.7  | Provisioning Systems                          | 13 |
|   | 6.8  | GAP ANALYSIS                                  | 14 |
| 7 | THR  | EATS  | 15 |
|   | 7.1  | Passive Threats                               | 15 |
|   | 7.2  | External (Active) Threats                     | 15 |
|   | 7.3  | Rogue Traffic                                 | 16 |
|   | 7.4  | MALWARE AND UNTRUSTED UPDATES                 | 16 |
|   | 7.5  | Denial of Service                             | 16 |
|   | 7.6  | SOCIAL ENGINEERING                            | 17 |
|   | 7.7  | Insider Threats                               | 17 |
|   | 7.8  | Supply Chain Threats                          | 17 |
|   | 7.9  | Integrator Threats                            | 18 |
| 8 | INF  | DRMATION TO SUPPORT AUTHORIZING OFFICIAL      | 18 |
| 9 | RISK | ( ASSESSMENT                                  | 19 |

| 10 | <b>CAMPUS W</b> | LAN SOLUTION REQUIREMENTS  | 19 |
|----|-----------------|--|----|
|    | 10.1 CSFC C     | Overall Solution Requirements                                      | 20 |
|    | 10.2 CSFC P     | PRODUCT SELECTION REQUIREMENTS                                     | 21 |
|    | 10.3 Confid     | GURATION REQUIREMENTS FOR THE END USER DEVICE (EUD)                | 23 |
|    | 10.4 Confid     | GURATION REQUIREMENTS FOR THE WLAN CLIENT (WC)                     | 25 |
|    | 10.5 Confid     | GURATION REQUIREMENTS FOR THE VPN CLIENT (VC)                      | 27 |
|    | 10.6 CONFIG     | GURATION REQUIREMENTS FOR BOTH VPN COMPONENTS (CR)                 | 27 |
|    | 10.7 CONFIG     | GURATION REQUIREMENTS FOR THE WLAN SYSTEM (WS)                     | 28 |
|    | 10.7.1          | Wireless System Physical Configuration                             | 29 |
|    | 10.7.2          | Wireless Infrastructure Authentication                             | 29 |
|    |                 | Wireless Authentication and Authorization Requirements             |    |
|    | 10.7.4          | Wireless Authentication Server to WLAN Client Requirements         | 30 |
|    |                 | ILTERING REQUIREMENTS  |    |
|    | 10.9 Confid     | GURATION OF THE VPN GATEWAY (VG)                                   | 32 |
|    | 10.10           | CONFIGURATION REQUIREMENTS FOR WIRELESS INTRUSION DETECTION SYSTEM |    |
|    | (WIDS           | 3) 32  |    |
|    | 10.11           | CONFIGURATION CHANGE DETECTION (CCD) REQUIREMENTS                  | 35 |
|    | 10.12           | REQUIREMENTS FOR INFRASTRUCTURE COMPONENT ADMINISTRATION (RA)      | 35 |
|    | 10.13           | NETWORK INTRUSION DETECTION SYSTEM (NIDS) REQUIREMENTS             | 36 |
|    | 10.14           | REQUIREMENTS FOR AUDITING (AU)                                     | 36 |
|    | 10.15           | REQUIREMENTS FOR KEY MANAGEMENT (KM)                               | 38 |
|    | 10.15.          | 1 General Key Management Requirements                              | 38 |
|    |                 | 2 IPsec VPN Key Management Requirements                            |    |
|    |                 | 3 WLAN Key Management Requirements                                 |    |
|    | 10.16           | Provisioning Requirements  |    |
|    | 10.16.          | 1 End User Device Provisioning Requirements                        | 40 |
| 11 | <b>GUIDANCE</b> | FOR USE AND HANDLING REQUIREMENTS                                  | 40 |
|    |                 | NCE FOR USE AND HANDLING REQUIREMENTS                              |    |
| 12 | COLUTION        | TESTING  | 42 |
| 12 | SOLUTION        | 1E51ING  | 43 |
| 13 |                 | RIA  |    |
|    | 13.1 WIRELE     | ESS CONNECTION ESTABLISHMENT PROTOCOLS                             | 44 |
|    | 13.2 WIRELE     | ESS INFRASTRUCTURE AUTHENTICATION PROTOCOLS                        | 46 |
|    | 13.3 EXTEND     | DED KEY USAGE EXTENSION CHECKING BY WLAN CLIENT                    | 47 |
|    | 13.4 EXTEND     | DED KEY USAGE EXTENSION CHECKING BY WLAN AUTHENTICATION SERVER     | 48 |
|    | 13.5 AUTHE      | NTICATION SERVER NAME CHECKING BY WLAN CLIENT                      | 48 |
|    | 13.6 CLIENT     | NAME CHECKING BY WLAN AUTHENTICATION SERVER                        | 49 |
|    | 13.7 Rоот (     | CERTIFICATE AUTHORITY CHECKING BY WLAN CLIENT                      | 49 |
|    | 13.8 AD HO      | c Mode   | 50 |
|    |                 | HORIZED SSIDs.   |    |
|    | 13.10           | AUTHENTICATION METHODS OTHER THAN EAP-TLS                          |    |
|    | 13.11           | AUTHORIZATION CHECK OF WLAN CLIENT CERTIFICATE                     |    |
|    | 13.12           | WLAN CLIENT AUTOMATIC ESTABLISHMENT                                |    |
|    | 13.13           | WLAN CLIENT CERTIFICATES   |    |

| 13.14             | WLAN AUTHENTICATION SERVER CERTIFICATE                  | . 53 |
|-------------------|---|------|
| 13.15             | WIRELESS SYSTEM CERTIFICATE                             | . 53 |
| 13.16             | WLAN Infrastructure Design Review                       | . 54 |
| 13.17             | WLAN Infrastructure Process Review                      | . 54 |
| 13.18             | WLAN CLIENT CERTIFICATE EXPIRATION NOTIFICATION         | . 55 |
| 13.19             | Pre-Shared Key Entropy Test                             | . 55 |
| 13.20             | WLAN CRYPTOGRAPHIC ALGORITHMS                           | . 55 |
| 13.21             | WLAN Bridging   | . 56 |
| 13.22             | Product Selection                                       | . 56 |
| 13.23             | END USER DEVICE CONFIGURATIONS                          | . 57 |
| 13.24             | IMPLEMENTATION OF GUIDANCE                              | . 59 |
| 13.25             | IMPLEMENTATION OF SOLUTION                              | . 59 |
| 13.26             | Provisioning of the EUD                                 | . 60 |
| 13.27             | COMPONENT ADMINISTRATION OF THE SOLUTION                | . 61 |
| 13.28             | AUDIT   | . 61 |
| 13.29             | CONFIGURATION CHANGE DETECTION                          | . 63 |
| 13.30             | CA CONFIGURATIONS                                       | . 64 |
| 13.31             | Use of Revoked Certificates                             | . 65 |
| 13.32             | Use of Certificates from Trusted CAs                    | . 65 |
| 13.33             | IMPLEMENTATION OF NIDS                                  | . 66 |
| 13.34             | IMPLEMENTATION OF VPN GATEWAY                           | . 66 |
| 13.35             | VPN COMPONENT CONFIGURATION                             | . 67 |
| 13.36             | IMPLEMENTATION OF PORT FILTERING                        | . 68 |
| 13.37             | IMPLEMENTATION OF WIDS                                  | . 68 |
| 13.38             | CA CONFIGURATIONS                                       | . 70 |
| APPENDIX A. HIG   | H LEVEL DESCRIPTION OF A END USER DEVICE INFRASTRUCTURE |      |
|                   | )N  | . 71 |
| APPENDIX B. GLC   | SSARY OF TERMS  | . 72 |
| APPENDIX C. ACR   | ONYMS LIST  | . 75 |
| APPENDIX D. REF   | ERENCES   | . 79 |
| APPENDIX E. EXA   | MPLE IAD APPROVAL LETTER FOR CAMPUS WLAN CAPABILITY     |      |
| PACKAGES .        |   | . 83 |
| ADDENINIY E CIIN  | MARY OF CHANGES TO REQUIREMENTS                         | Q/I  |
| AFFLINDIA F. JUIV | TIMENT OF CHANGES TO REQUIREIVES                        | . 04 |

# **TABLE OF FIGURES**

| Figure 4-1. Campus WLAN Infrastructure for Classified                | 4  |
|--|----|
| Figure 4-2. Campus WLAN Infrastructure for Classified                | 6  |
| Figure 5-2. Campus WLAN End User Device Architecture                 | 8  |
| TABLE OF TABLES  |    |
| Table 1 CSfC Overall Solution Requirements                           | 20 |
| Table 2 Product Selection Campus WLAN Architecture Requirements      | 21 |
| Table 3 WLAN Solution Component Selection Restrictions               | 23 |
| Table 4 Applicable CSfC Component Lists for the Campus WLAN Solution | 23 |
| Table 5 WLAN End User Device (EUD) Requirements                      | 24 |
| Table 6 WLAN Client (WC) Configuration Requirement                   | 25 |
| Table 7 Wireless Link Requirements                                   | 26 |
| Table 8 Approved Interim Algorithms                                  | 26 |
| Table 9 Approved Suite B Algorithms                                  | 27 |
| Table 10 VPN Client (VC) Configuration Requirements                  | 27 |
| Table 11 Configuration Requirements for Both VPN Components          | 27 |
| Table 12 Wireless System Configuration Requirements                  | 29 |
| Table 13 Wireless Infrastructure Authentication Requirements         | 29 |
| Table 14 Wireless Authentication and Authorization Requirements      | 30 |
| Table 15 Wireless Authentication Server to WLAN Client Requirements  | 30 |
| Table 16 Port Filtering (PF) Requirements                            | 31 |
| Table 17 VPN Gateway (VG) Requirements                               | 32 |
| Table 18 Wireless IDS (WIDS) Configuration Requirements              | 32 |
| Table 19 Configuration Change Detection (CCD) Requirements           | 35 |
| Table 20 Component Administration (RA) Requirements                  | 35 |
| Table 21 Network Intrusion Detection System (NIDS) Requirements      | 36 |
| Table 22 Auditing (AU) Requirements                                  | 36 |
| Table 23 General Key Management Requirements                         | 38 |
| Table 24 IPsec VPN Key Management Requirements                       | 39 |
| Table 25 WLAN Key Management Requirements                            | 39 |
| Table 26 End User Device Provisioning Requirements                   | 40 |
| Table 27 Guidance for Use and Handling Requirements                  | 42 |
| Table 28 Testing Requirement   | 44 |

#### 1 INTRODUCTION

The Commercial Solutions for Classified (CSfC) program within the National Security Agency (NSA) Information Assurance Directorate (IAD) uses a series of Capability Packages to provide configurations that will allow customers to independently implement secure solutions using layered Commercial Off-the-Shelf (COTS) products. The Capability Packages are vendor-agnostic and provide high-level security and configuration guidance for customers and/or Solution Integrators.

IAD is delivering a generic CSfC Campus IEEE 802.11 Wireless Local Area Network (WLAN) Capability Package to meet the demand for commercial End User Device (i.e., tablet and laptop computers) to access secure enterprise services over a campus wireless network. These algorithms, known as Suite B algorithms, are used to protect classified data using layers of COTS products. Campus WLAN Capability Package Version 1.1 enables customers to implement layered encryption between a Red Network site and End User Devices (EUDs). This Capability Package takes lessons learned from two proof-of-concept demonstrations. These demonstrations included a layered use of COTS products for the protection of classified information. The CSfC Campus IEEE 802.11 WLAN Capability Package Version 1.1 supersedes the Campus IEEE 802.11 WLAN Capability Package Version 1.0, dated 20 August 2013.

#### 2 PURPOSE OF THIS DOCUMENT

This Capability Package provides reference architecture and corresponding configuration information that allows customers to select COTS products from the CSfC Components List for their Campus WLAN solution and then to properly configure those products to achieve a level of assurance sufficient for protecting classified data while in transit. As described in Section 10.2, customers must ensure that the components selected from the CSfC Components List will permit the necessary functionality for the selected architecture. Throughout this document, requirements imposed on the Campus WLAN solution, to ensure proper implementation, are identified by a label consisting of the prefix "WLAN," a two-letter category, and a sequence number (e.g., WLAN-KM-11). To successfully implement a solution based on this Capability Package, all Threshold requirements, or the corresponding Objective requirements, must be implemented, as described in Section 10.

Customers who want to use a variant of the solution detailed in this Capability Package must contact NSA to determine ways to obtain NSA approval. Additional information about the CSfC process is available on the CSfC web page (www.nsa.gov/ia/programs/csfc\_program).

#### **3** USE OF THIS DOCUMENT

Solutions compliant with this Capability Package must be registered with NSA/IAD to be considered approved by IAD. Once registered, a signed IAD Approval Letter will be sent to the customer validating that their solution is compliant with the Campus WLAN Capability Package. Registrations must be renewed annually to ensure fielded CSfC solutions remain compliant with the current version of the Capability Package.

Please provide comments on usability, applicability, benefits and/or shortcomings to your NSA/IAD Client Advocate and the Campus IEEE 802.11 WLAN Capability Package maintenance team at Wi-Fi@nsa.gov.

The following Legal Disclaimer relates to the use of this Capability Package:

This Capability Package is provided "as is." Any express or implied warranties (including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose) are disclaimed. In no event shall the United States Government be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services, loss of use, data, or profits, or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this Capabilities Package, even if advised of the possibility of such damage.

The User of this Capability Package agrees to hold harmless and indemnify the United States Government, its agents and employees from every claim or liability (whether in tort or in contract), including attorneys' fees, court costs, and expenses, arising in direct consequence of Recipient's use of the item (including, but not limited to, claims or liabilities made for injury to or death of personnel of User or third parties, damage to or destruction of property of User or third parties, and infringement or other violations of intellectual property or technical data rights).

Nothing in this Capability Package is intended to constitute an endorsement, explicit or implied, by the U.S. Government of any particular manufacturer's product or service.

#### 4 DESCRIPTION OF CAMPUS IEEE 802.11 WLAN SOLUTION

The Solution described within this Capability Package is supported by the use of wireless devices to access sensitive data and enterprise services while minimizing the risk when connecting to existing Government enterprise networks. Government-managed campus-area wireless networks provide controlled connectivity between mobile users and the broader Government enterprise. The term "Campus" is used in this document to refer to any area which is physically protected to the classification level of the red network data. This physical area includes secure facilities and tactical environments when the physical controls are deemed appropriate by the Authorizing Official.

Figure 4-2. depicts at a high level the Campus IEEE 802.11 WLAN solution within the context of the basic segments of the Campus WLAN architecture.

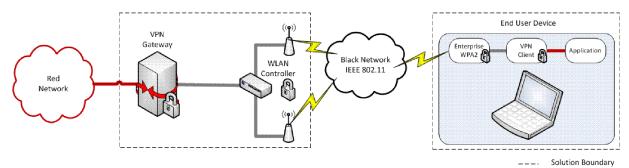


Figure 4-2.

Composed, layered solutions are the basis for the secure use of End User Devices and commercial components for access to Government enterprise services and data. Layers of commercial encryption, layers of authentication and authorization, boundary protection, possible hardening of devices, and End User Device provisioning/management all contribute to overall system security.

The following are the overarching themes for secure Campus WLAN capabilities:

- Employ layered Data-In-Transit protection to tunnel traffic from the End User Device to the enterprise boundary.
- Ensure that all service requests and user traffic from a End User Device are mediated through the Red Network.
- Locate the bulk of security functionality and trust in the enterprise.
  - Provision and manage devices to establish and maintain secure operations.
  - Authenticate devices prior to authorizing network and service access.
  - Provide strong boundary protection to limit risk to Government resources.
- Wherever possible, harden commercial devices to protect integrity and reduce risks.

In order to adequately protect sensitive information using commercial devices, the following cryptographic principles apply:

- For wireless transmission of data on Black networks, two layers of approved commercial cryptography will be required. The inner layer shall be provided by Internet Protocol Security (IPsec) which establishes a secured path between the EUD and the Red Network. In this Capability Package the outer layer is the Wi-Fi Protected Access 2 (WPA2) encryption with the specified algorithm requirements.
- Government-issued device certificates or certificates issued via an NSA-approved commercial managed PKI service shall be used for mutual authentication in both layers.
- The systems providing each layer of encryption should be entirely independent of each other (e.g. application components and libraries).

#### 4.1 Networks

There are network segments within the architecture in which the data is unencrypted, protected with only one layer of data-in-transit encryption and protected with two layers of data-in-transit encryption. For clarity, these network segments are described by their logical location and the level of protection they provide. The following terms are used throughout this document:

#### 4.1.1 Red Network

A Red network contains unencrypted classified data and is logically located behind an Inner VPN Gateway. The networks connected to End User Devices through the Campus WLAN solution are Red networks. Red networks are under the control of the solution owner or a trusted third party. The Red network may only communicate with EUDs through the Campus WLAN solution if the EUDs operate at the same security level.

#### 4.1.2 Gray Network

A Gray network contains classified data that has been encrypted once. The network between an Inner VPN Gateway and the Wireless System is a Gray network. Gray networks are under the control of the solution owner or a trusted third party. Gray networks are either physically or cryptographically divided into two sub-networks, as follows:

- Gray Management network The part of a Gray network that contains the management functions to run components supporting the Outer layer of WPA2, including the Outer tunnel Certificate Authority (CA) and the Outer admin and audit server functions.
- Gray Data network The part of a Gray network that carries data between Inner VPN Gateway and the Wireless System.

#### 4.1.3 Black Network

A Black network contains classified data that has been encrypted twice. The wireless network between the End User Device and the Wireless System in which data is protected with two layers of encryption (the IPsec and the WPA2 layers) is a Black network. Black networks are not necessarily (and often will not be) under the control of the solution owner or can be interfered with by external third party actors.

# 4.2 Campus IEEE 802.11 WLAN Solution Architecture

The Campus IEEE 802.11 WLAN CSfC solution addresses the need to protect classified information as it travels over-the-air between a WLAN-enabled EUD and a WLAN Infrastructure attached to a wired network of the same classification level. The solution also addresses the risks introduced to the red network by providing a wireless interface. In the absence of a NSA-approved Data at Rest (DAR) solution, the EUD shall be physically and administratively protected at the classification level of the red network it is accessing.

As seen in Figure 4-2., the architecture utilizes two layers of cryptography: one WPA2 and one IPsec. Each layer should meet the requirements of CNSS Policy (CNSSP) No. 15, "National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems," dated 1 October 2012. To implement a WLAN solution that uses two layers of IPsec encryption, you have the option of complying and registering with the VPN Capability Package version 2.0 instead of this capability package.

Figure 4-2. depicts how these components are implemented in accordance with the Campus WLAN Capability Package.

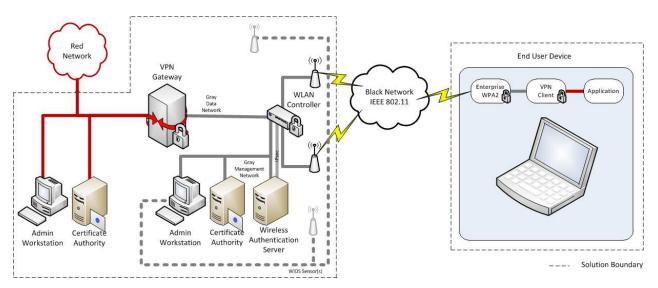


Figure 4-2. Campus WLAN Infrastructure for Classified

# 4.3 Interactions with Enterprise Services

The two layers of encryption (WPA2 and IPsec) required by this Capability Package result in the creation of nested secure tunnels that carry Internet Protocol (IP) packets between the End User Device and the Red network. The VPN Gateway is the endpoint of the inner tunnel on the infrastructure side. Integration with the back-end red network on the unencrypted side of the inner tunnel is outside the scope of this Capability Package, but this section identifies some best practices. Appropriate organizational policies and directives should be consulted for definitive information.

The Campus WLAN solution described in this Capability Package is application-agnostic in that it provides an end-to-end path for IP packets between the EUD and the Red Network without regard to what those IP packets contain. Enterprise services may or may not depend on the ability of the EUD to provide local non-volatile storage for user data, configuration data, or state information (e.g., persistent cookies).

The user authentication services described in Section 4.3 may be implemented within application gateways and proxies that provide boundary protection services between the VPN Gateway and backend enterprise application services. These boundary protection services may include application protocol validation and malicious code detection, and may forward the authenticated user identity to the application services.

**Boundary Protection:** Analogous to the guidance for remote access to unclassified networks, each packet emerging from the tunnel should be analyzed to the same degree as an un-tunneled packet arriving from an external network. The boundary protections at the tunnel exit point should include an Intrusion Detection or Prevention System (IDS or IPS) to detect network attacks followed by one or more filters to limit access to enterprise resources. The minimum suggested configuration is an IDS/IPS

combined with port filtering. To provide more protection, application-level filtering may be added to verify that application protocols are well-formed and do not contain embedded malicious code.

**Authentication and Authorization:** The WLAN and VPN Gateway only authenticate End User Device identities using device certificates. It is recommended (and may be required by the Authorizing Official) that the End User Device user be authenticated prior to granting access to back-end application services. This verification should be centralized and occur as close to the network edge as possible.

**Guidance:** The following references provide useful guidance for securing remote access to enterprise resources for the Department of Defense (DoD). This guidance for securing remote access should be applied within the context of the classified network for which a wireless connection is provided.

- Secure Remote Computing (SRC) Security Technical Implementation Guide (STIG), Defense Information Systems Agency (DISA)
- Network Infrastructure Technology Overview, DISA
- Remote Access Policy STIG, DISA
- Remote Access Server (RAS) STIG, DISA

#### **5 END USER DEVICE**

The EUD is a commercial tablet, laptop computer, or similar computing device that supports Wi-Fi connectivity options. It may run applications that make use of local processing or local persistent storage ("thick client") or "thin client" applications such as remote desktop clients. When running a "thin client" application, user data may be written to non-volatile memory (for example, to a page file). As a result, the overall EUD cannot be considered a thin client device and must be protected at all times in accordance with policy applicable to the classification level of the user data it processes. In the absence of a NSA-approved DAR solution, the EUD shall be treated as classified device at all times.

Figure 5-2 shows the software architecture of a typical EUD. The VPN client and WLAN client run as operating system processes and exist to perform authentication and key establishment for the IPsec module and WPA2 driver respectively. Each client shall use a different user-mode cryptographic library to meet CSfC diversity requirements. As depicted, the VPN client is using its own cryptographic library, whereas the WPA2 client is using a user-mode cryptographic library supplied as part of the operating system. Encryption of the user data is often performed directly in the kernel for performance reasons. If the VPN client and WLAN client both use the operating system's built-in kernel-mode cryptographic library, this results in loss of cryptographic diversity even when different user-mode libraries are used for authentication and key establishment. Candidate products should be carefully evaluated to ensure the cryptographic independence of the WLAN and VPN Clients as required by CSfC.

# 5.1 End User Device (EUD) Protection

The EUD consists of the hardware and software components (OS, VPN client, WLAN client, and applications) that provide a variety of security services.

The operating system of the EUD is responsible for providing the following security functions to enable secure connections to the Red Network and to ensure that the device operates under known, authorized conditions:

• EUD protection capabilities, including:

- System configuration—initial provisioning to remove or disable non-essential services and install required software.
- Port Filtering-Restrict traffic to authorized address ranges and protocols
- Device monitoring—notification and logging of security faults with cessation of operations for critical events.
- Local authentication—separate layers of authentication to provide access to the device and to the enterprise.
- Local key and certificate management for the VPN and WLAN clients and other applications.
- VPN and WLAN clients—one of these may be completely implemented by the operating system or responsibility may be shared with third-party components that perform authentication and key establishment functions.

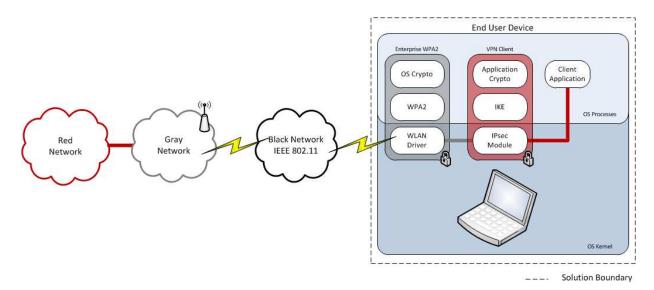


Figure 5-2. Campus WLAN End User Device Architecture

#### 5.2 WLAN Client

The WLAN Client is a software application that provides management and control of the IEEE 802.11 wireless connection. The products chosen to implement the WLAN Client services shall provide a base level of protection and shall be able to interoperate with products from other vendors. The WLAN Client automatically establishes the IEEE 802.11 WPA2 tunnel between the End User Device and the Wireless System using Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) over IEEE 802.1X to pass Public Key device certificates for mutual authentication between the WLAN Client and WLAN Authentication Server.

#### 5.3 VPN Client

The VPN Client is a software application running on the End User Device. The products chosen to implement the VPN services shall provide cryptographic and functional services that meet or exceed the

requirements listed in Section 10 for the VPN Client, and they should ideally also support interoperability with products from other vendors.

The VPN Client establishes an IPsec tunnel to the VPN Gateway. The VPN Client first performs an IKE exchange with the VPN Gateway to authenticate both parties and exchange session keys for the IPsec tunnel. Authentication is performed via mutual authentication of Public Key device certificates. When IKE completes, the IPsec tunnel is secured using the Encapsulating Security Payload (ESP).

# 5.4 Client Applications

Client applications interact with application services located on the Red network to provide functionality to end users. Client applications may be "thin" or "thick" in terms of whether they store data in local non-persistent storage.

# 5.5 Gap Analysis

- Currently, the EUD cryptographic libraries and randomizers utilize the same processor. The vendor diversity and process separation available in today's EUDs and required by this Capability Package has been determined to provide adequate independence for current solutions. Two layers are considered independent when:
  - The implementations of each layer are from different vendors and are not derived from a common codebase.
  - The implementations of each layer do not share cryptographic functions (i.e., a shared cryptographic library or source of randomness).
  - The operation of one layer does not influence the operation of the other layer except as defined by the interface between them (i.e., covert channels are eliminated).
- Tablets may have limited management capabilities in comparison to laptops:
  - Non-essential services cannot be removed or permanently disabled.
  - Sufficient device monitoring is not currently available for tablets. First, some devices do not support local access to audit logs. In addition, remote monitoring services could be provided by End User Device Management (MDM) software in the future. Unfortunately, some devices currently require Internet access in order to implement an MDM solution, preventing MDM use with the Campus IEEE 802.11 WLAN solution. Furthermore, most of those that do not require Internet access do not have sufficient kernel-level Application Program Interfaces (APIs) available for the monitoring service.
  - Updates to the tablet software cannot be performed over-the-air and in some cases cannot be performed at all without Internet access. Due to device classification, tablets may not be connected to the Internet in order to perform updates.
  - User and administrator actions on some tablets cannot be distinguished.
  - Administrators have limited capabilities for locking settings and preventing users from changing settings. This limitation is particularly damaging with regard to user access to wireless network settings.
  - Unwanted root certificates (preloaded) from some tablets cannot be removed.

- Many implementations are not able to use device certificates issued by different Certificate
   Authorities for the WLAN client and VPN client without separate certificate stores. Virtualization
   may be functionally necessary to create these two stores and is sufficient for providing
   independence and separation of the two layers. However, virtual machines are not, from a
   security perspective, necessary to provide independence of the two layers.
- Few tablet operating systems sufficiently protect the private keys in the native certificate store. Furthermore, most do not support Elliptic Curve Digital Signature Algorithm (ECDSA) certificates in the native certificate store. Thus, Suite B capable WLAN and VPN clients have an application-layer certificate store. These application stores often do not provide basic protections such as encrypting the private keys or preventing manipulation by other applications. Both native and application certificate stores should be implemented with key generation inside an approved Federal Information Processing Standard (FIPS) 140-2 compliant component and with an Application Programming Interface (API), such as one meeting Public Key Cryptography Standard (PKCS) #11,that prevents the private key from leaving the cryptographic boundary of the store. To enable use of the devices outside a secure facility, future requirements may include token-based certificates or password protection of the private keys stored on the device.
- The Wireless Fidelity (Wi-Fi) Alliance is an industry standards body that certifies Wi-Fi-enabled products against the IEEE 802.11 and Transport Layer Security (TLS) standards to ensure interoperability of vendor products. The Alliance's WPA2 certification requires an EAP method for authentication, for which TLS 1.0 is suggested as a minimum. TLS 1.0 allows Elliptic Curve Cryptography but does not support the Secure Hash Algorithm 2 (SHA-2) family which is what is required to meet the Suite B objectives of this Capability Package. The Wi-Fi alliance does not currently recommend or test for TLS 1.2.
- At the time of this publication, commercial Data at Rest (DAR) products are not approved to
  protect classified information. Absent an NSA-approved DAR solution, EUDs must be handled as
  classified at all times, even when powered off.
- A trusted boot capability based on a hardware root-of-trust to interact with a Network Access
  Controller (NAC) in the Red Network is needed to attest to the hardware and software integrity
  of the EUD. Not all EUDs support trusted boot capabilities, and any trusted boot capabilities
  currently developed may not allow interaction with a network controller within the enterprise.

#### 6 CAMPUS WLAN ARCHITECTURE COMPONENTS

# 6.1 Wireless System

In the context of this solution, the Access Points (APs), and the WLAN Controller compose the "Wireless System." These components are grouped together in this document to maintain vendor neutrality; there are a variety of wireless system implementations across the vendor community.

An AP is the media converter providing a link between the WLAN Client and the wired switch. The level of functionality contained within the APs is vendor-dependent. Some solutions utilize "smart" or "thick" APs which incorporate a significant amount of functionality, including cryptographic operations. In this case, the APs would be considered part of the gray network. Whereas other solutions implement "thin" APs that merely perform the wireless/wired media conversion and push all functionality to the WLAN

Controller. In this case, the APs would be considered part of the Black network. Some vendors may produce both types of solution. If WPA2 terminates on APs rather than on the WLAN Controller, then the connection between the APs and the WLAN Controller should be encrypted in a manner leveraging the CAPWAP standard. If WPA2 terminates on the WLAN Controller, then the WPA2 encryption protects the connection between the APs and the WLAN Controller.

The Wireless System shall be capable of initiating and terminating multiple IEEE 802.11 cryptographic tunnels to and from numerous Wireless Clients. It shall also be capable of translating EAP-TLS over IEEE 802.1X messages to EAP-TLS over Remote Authentication Dial in User Service (RADIUS) messages to pass authentication information between the WLAN Client and WLAN Authentication Server. As part of this exchange, a Pairwise-Master Key (PMK) is negotiated between the WLAN Client and the WLAN Authentication Server. The WLAN Authentication Server passes the PMK to the Wireless System over an IPsec tunnel. The Wireless Controller and the WLAN Client use the PMK to negotiate a session key to protect the subsequent user traffic exchanged between the WLAN Client and the Wireless System. The Wireless System should operate on its own separate hardware and/or virtual device(s); depending on the vendor implementation, as mentioned above. This separation may include isolating the switches and wiring between the APs and the controller from any existing network. At the very least, the Wireless System and the VPN Gateway shall operate on separate hardware. Since the wireless system is deployed between the Black network and the Gray management network, it is essential to implement port filtering on the wireless system's Gray network interface to prevent unauthorized traffic. Traffic should be restricted to those stated in Section 10.7.2.

# 6.2 Wireless Intrusion Detection System

An IEEE 802.11 Wireless Intrusion Detection System (WIDS) consists of a group of sensors (preferably some dedicated) and a central controller working together to provide 24/7 monitoring of the wireless spectrum to detect unauthorized WLAN activity. The system can either be stand-alone or integrated into the Wireless System. For the stand-alone case, ideally, information between the sensors and the controller will pass over a separate network dedicated to the WIDS, but an acceptable option is to connect the sensors over a virtual LAN established over the same wired network as used by the Wireless APs. For an integrated WIDS, whether the sensors can be placed on the Wireless network or must be placed on the Gray network depends on the vendor's implementation.

#### 6.3 WLAN Authentication Server

WLAN Authentication Server performs device authentication during the IEEE 802.1X exchange. The Wireless Client and WLAN Authentication Server perform an EAP-TLS exchange using the IEEE 802.1X protocol, with the wireless system acting as a pass-through. As part of this exchange, a shared session key is negotiated between the WLAN Client and the WLAN Authentication Server. The WLAN Authentication Server passes this key to the Wireless System over an IPsec tunnel to protect the subsequent user traffic exchanged between the WLAN Client and the Wireless System. The WLAN Authentication Server should operate on a separate hardware device from the Wireless System.

#### 6.4 Administration Workstations

The Wireless System, WLAN Authentication Server, and the WLAN client shall have administration workstation on the Gray Management network that allows for maintaining, monitoring, and controlling all security functionality for those devices. The administration devices for the VPN are located on the Red network. These administration devices shall also allow for logging and configuration management,

as well as reviewing audit logs. Given the architecture of the solution, there are distinct administration networks for the WLAN and VPN devices. Layer 3 routing between management and data networks shall be prohibited to maintain strict separation between management and data traffic.

Administration Workstations shall be dedicated for the purposes given in the Capability Package, and shall not be used to manage any non-CSfC solutions. As such, a dedicated virtual machine on an administration device used for non-CSfC solution cannot be used to manage CSfC solutions.

A Network-based Intrusion Detection System (NIDS) should be deployed on the Gray network. The NIDS must be regularly updated with attack signatures. It is recommended that a separate NIDS also be deployed on the Red network to monitor tunneled IP traffic being decrypted by the VPN Gateway.

Infrastructure components (servers and workstations) should be configured with Host-based IDS (HIDS) software in accordance with local policy.

# 6.5 Certificate Authority

Two separate Certificate Authorities (CA's) support the two layers of data-in-transit encryption (WPA2 and IPsec) in this Capability Package. Each CA provides independent keys to the WLAN and VPN clients respectively, and the corresponding infrastructure components:

- End User Device registration services.
- Certificate issuance services.
- Certificate renewal services.
- Certificate Revocation Services (via Certificate Revocation Lists (CRLs) and/or Online Certificate Status Protocol (OCSP).

Deploying two Certificate Authorities decreases the risk to the infrastructure as they provide two independent points of failure. In addition, because they provide a signer for key pairs these Certificate Authorities provide the third party trust between the users of certificates. Both the End User Device clients and the infrastructure components are issued certificates. Each has a critical role to play in verifying the trust of the other party as they connect in the wireless environment. The WLAN Authentication Server checks certificate revocation status prior to allowing a device to connect to the Gray network. Similarly, the VPN Gateway checks certificate revocation status prior to allowing a device to connect to the Red network.

Certificate revocation information should be made available to, and checked by, infrastructure components. The certificates for any compromised EUD shall be revoked and/or removed from the certificate whitelist and new CRLs are issued. As private keys on infrastructure components are comparatively secure, the cost of making certificate revocation information available to EUDs may outweigh the benefit of doing so.

Each CA used in the solution shall have an approved Certificate Policy/ Certificate Practice Statement (CP/CPS) that addresses certificate generation, handling, distribution, storage, destruction, and key recovery and compromise recovery. Refer to NIST SP 800-57 for guidance.

The CA for the WLAN devices shall be located in the Gray management network and the CA for VPN devices shall be located in the Red network. If Enterprise CA's are available, they should be utilized. Otherwise a locally managed CA will need to be deployed requiring that a CA product be selected from the CSfC component list.

Each CA shall operate on a dedicated machine, but the CAs may be operated as virtual machines (i.e., the WLAN Authentication server and the WLAN CA may be Virtual Machines (VMs) on the same hardware platform).

#### 6.6 VPN Gateway

The VPN Gateway is an integral part of the security of the Campus IEEE 802.11 WLAN solution and is located on the gray interface of the secure wired network. Port filtering rules shall be implemented in order to prevent unauthorized traffic from reaching the Enterprise services. The VPN Gateway performs cryptographic functions related to establishing and maintaining the IPsec tunnels. It is responsible for authenticating the device certificate of the EUD's VPN Client, including checking for certificate revocation information during the IPsec VPN tunnel establishment. The VPN Gateway shall operate on its own separate hardware device.

# **6.7 Provisioning Systems**

Initial provisioning of campus End User Devices will be performed using enrollment capabilities hosted in the Red Network and leveraging the WLAN and VPN CAs. To support different device types, it may be necessary to support both a wireless and wired connection capabilities to the End User Device being provisioned. Since keying and secure applications are needed to connect to the operational wireless system have not yet been established, wireless provisioning connectivity must be performed on a separate wireless system in a shielded enclosure. The provisioning process includes assigning identifiers to the devices, installing required applications, configuring the device's policy and settings (especially WPA2 and IPsec settings), and loading certificates and keying material. Prior to provisioning devices, configuration profiles are created and required device applications are obtained.

Initial provisioning (for all device types) should include—note that a specific sequence is not implied:

- Device registration. Collect identifying information from the End User Device, assign
  Government device identities for the Gray and Red domains, and update data stores (directory, inventory, and/or authorization) to include new End User Device.
- 2. **Profile and settings configuration**. Load configuration profiles (within the limitations of what is supported by each device type) that implement policies on allowed and disallowed services (such as Bluetooth) and user authentication parameters (such as password length and when to lock the device). Supply other settings such as network parameters.
- 3. **Application installation**. Load required applications including the VPN client and enterprise client applications (there is no current support for an online application store so all applications should be loaded during initial provisioning). If possible, unneeded applications should be removed from the device.
- 4. **Certificate request and issuance**. Using the assigned Government device identifiers, connect to the Gray network, request certificates from the WLAN CA, and load received material into the End User Device. Disconnect the device from the Gray network, connect to the Red network, request certificates from the VPN CA, and load received material into the End User Device.

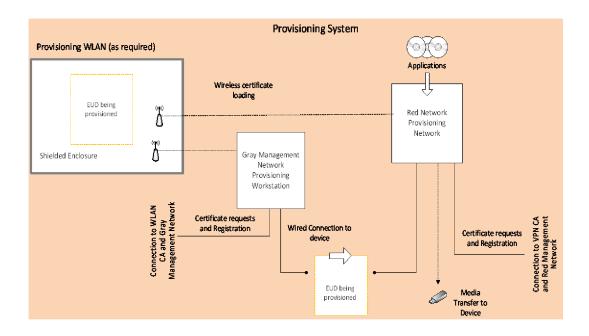
Depending on the capabilities of the EUD, the device either connects and interacts with the CAs in order to be issued certificates, or the certificates are generated and loaded onto a device storage medium from a Provisioning workstation for transfer to the End User Device. There will also be differences based on whether the End User Device generates and provides a private key for the certificate or is issued one

from the CA (more secure handling and transfer is required for the latter case). Finally, some devices may require that certificate provisioning be performed using a wireless connection. In the event that a device can only support wireless certificate provisioning, the certificate provisioning must be performed in a shielded enclosure.

shows a possible configuration of Provisioning systems including a shielded enclosure with isolated wireless connectivity.

Once the End User Device is properly configured and certificates/keying material is in place, it is ready to be issued to a user with the final steps of establishing user login and associating the user with the device in the registration data. Once the device is connected to the Red network, the device is classified.

If the implementing organization already has provisioning capabilities for classified EUDs, then they will need to be modified and augmented to support device registration with the Gray network and certificate issuance from the WLAN and VPN CAs. If this is the first use of classified EUDs within the implementing organization, then this section provides an overview of the services and systems needed to provision them.



#### Figure 6-1. Provisioning and Key Loading for Campus WLAN

# 6.8 Gap Analysis

- The recent publication of the IEEE 802.11ac specification addresses a gap which previously limited WLAN encryption is to 128-bit Advanced Encryption Standard (AES-128) Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP) mode because the IEEE 802.11 Specification does not support any other cipher modes. CCMP mode and Galois/Counter Mode Protocol (GCMP) are both approved for use in Wireless LAN Access Systems implementing the IEEE 802.11ac standard, which enables the use of 256-bit AES keys.
- Like WLAN clients, WLAN Authentication servers do not support TLS 1.2 for EAP-TLS.
- Most WIDS currently do provide enough flexibility in creating custom intrusion event signatures. The
  most flexible way to do this would be to allow the administrator to combine filters on every field in a
  IEEE 802.11 frame, including those encapsulating EAP-TLS, using Boolean logic.
- WIDS do not perform advanced statistical analysis of the monitored network. The system should take advantage of modern machine learning techniques to perform statistical analysis of the wireless traffic of individual devices and of the monitored network as a whole.
- The provisioning capabilities of some EUDs are limited; thus, the provisioning process described above does not scale well. Furthermore, a subset of these EUDs requires wireless provisioning.

#### 7 THREATS

This section details how the required components work together to provide overall security in the solution. Figure show the solution boundary of the Campus WLAN.

An assessment of security was conducted on the architecture described in this Capability Package while making no assumptions regarding use of specific products for any of the defined components. There are several different threats to consider when evaluating the risk of transporting data over secure or unsecure networks. By examining these threats, the organization can have a better understanding of the risks they are accepting by implementing the solution and how these risks affect the Confidentiality, Integrity, and Availability of the network, systems, and data.

#### 7.1 Passive Threats

These threats refer to internal or external actors attempting to gain information from the network without changing the state of the system. Threat actions include collecting or monitoring traffic (e.g., traffic analysis or sniffing the network) passing through a network in order to gain useful information through data analysis.

The security against a passive attack targeting the data in transit across the Black network is provided by the IPsec and WPA2 layers. To mitigate passive attacks, two layers of Advanced Encryption Standard (AES) are employed to provide confidentiality for the solution. Use of AES is approved to protect classified information, meeting IAD guidance for adequate confidentiality. The two layers that are used

to set up the tunnels must be independent in a number of ways (see Section 9). Due to this independence, the adversary should not be able to exploit a single cryptographic implementation to compromise both tunnels.

# 7.2 External (Active) Threats

These threats refer to outsiders gaining unauthorized access to a system or network, exfiltration of sensitive Red network data, or degradation of availability of the system or network. Threat actions include introducing viruses, malware, or worms with the intention to compromise the network or exfiltrate data, or to analyze the architecture of the network or system for future attacks. Adversaries could gain access to the Wireless System or EUD, and then exploit or compromise other devices on the network. Denial of Service (DoS) or Distributed DoS (DDoS) attacks compromise availability of the system, degrading/disrupting secure communication across the Black network. Further external threat actions would include social engineering attacks to assist attackers with gaining additional access to a network for the purpose of compromising a system or network, traffic injection or modification attacks, or replay attacks.

# 7.3 Rogue Traffic

One method for detecting rogue traffic from an external attack as it attempts to pass through WLAN or VPN Components is by having the port filtering native to each component enabled and configured to audit and log any traffic that is not of the format described in the configuration. It is required that the port filtering be set up to block the following:

- 1) any traffic not coming from or going to an IP address on the network at the other site
- 2) traffic not contained in IP packets other than control plane protocols needed for network operation and approved by AO/DAA policy
  - 3) traffic going to unexpected ports

This will allow the Auditor(s) and/or the Security Administrator(s) to detect whether the Wireless System has been breached, thus providing an early warning of a potential intrusion. It will also provide detection of Wireless System mis-configuration.

Another method for detecting a potential intrusion into the solution is requiring automated configuration change detection on the Red and Gray Management networks to ensure the component configurations are not changed without the knowledge of the Auditor and Security Administrator. The Auditor also ensures through the audit logs that all configuration changes are valid. This will counter attacks that take advantage of component mis-configurations.

EUDs are protected from rogue traffic through the use of traffic filtering rules configured on its interfaces connected to the Black network to drop any traffic not necessary for connecting to the Outer VPN Gateway.

# 7.4 Malware and Untrusted Updates

The Administration Workstations and CAs for the Red network shall be distinct from the Administration Workstations and CAs for the Gray network. This separation will minimize the potential of malware on a single device impacting components supporting both the WPA2 and IPsec tunnels.

Each individual component of this solution has the capability to perform trusted updates through verification of a signature or hash to ensure that the update is from a reliable source, such as signed by the vendor. This mitigates threats of malicious users trying to push updates or code patches that affect the security of the component (and therefore system). The source of all updates and patches should be verified before installation occurs.

#### 7.5 Denial of Service

DoS attack risks cannot be completely mitigated. The solution requires dropping all packets that are not Internet Key Exchange (IKE), Encapsulating Security Payload (ESP), WPA2, and EAP-TLS or approved control plane protocol traffic on the appropriate interfaces, which significantly reduces the potential of flooding attacks. Other mitigations are acceptable and up to the AO/DAA to approve their use.

A single component failure is likely to result in a DoS condition. One assumption underlying this solution is that high assurance of availability is not required. If availability is critical for the customer, network redundancy can support further DoS protection as well as having procedures for response when loss of availability is detected.

# 7.6 Social Engineering

It is the responsibility of the customer to define the appropriate policies and training necessary to protect against Social Engineering attacks. In addition, these types of attacks generally take advantage of other attacks detailed in this section and already discussed.

#### 7.7 Insider Threats

These threats refer to an authorized or cleared person or group of people with access, physical or logical, to the network or system who may act maliciously or negligently, resulting in risk exposure for the organization. This threat could include poorly trained employees, curious employees, disgruntled employees, escorted personnel who gain access to the equipment, dishonest employees, or those that have the means and desire to gain escalated privileges on the network.

Threat actions include insertion or omission of data entries that result in loss of data integrity, unintentional access to an unauthorized system or network, willingly changing the configuration of an EUD, unwillingly or unknowingly executing a virus or malware, intentionally exposing the network and systems to viruses or malware, cross-contaminating a system or network with data from a higher classification to a lower classification (e.g., Secret data to Unclassified network or system), or malicious or unintentional exfiltration of classified data. Typically, the threat from insiders has the potential to cause the greatest harm to an organization, and insider attacks are also the hardest to monitor and track.

To mitigate insider threats, separation of roles within the solution is required. In addition, logging and auditing of security critical functionality is required. Also, strong authentication of the Security Administrator and Auditor are required for access to ensure accountability of these individuals. Finally, outbound filters on components are configured to look for traffic leaving the internal network that does not go through the tunnels. In scenarios that need additional assurance, an optional IDS could be deployed on the Gray network to help identify whether there is a failure, mis-configuration, or attack on the Inner or outer components.

# 7.8 Supply Chain Threats

A critical aspect of the U.S. Government's effectiveness is the dependability, trustworthiness, and availability of the information and communication technology (ICT) components embedded in the systems and networks upon which the ability to perform their missions rely. The supply chain for those ICT components are the underpinnings of those systems and networks and supply chain attacks are attempts to proactively compromise those underpinnings.

Unfortunately, the supplier cannot always provide guarantees of a safe delivery of a component; they are only able to provide assurances based on their reliance of established procedures and processes they have developed. In a single change of hands, the component may be introduced to potential threats and compromises on many levels.

The supply chain threat refers to an adversary gaining access to a vendor or retailer and then attempting to insert or install a modification or a counterfeit piece of hardware into a component that is destined for a U.S. Government customer in an effort to gain information or cause operational issues. This threat also includes the installation of malicious software on components of the solution. This threat is difficult to identify and test, and is increasingly more difficult to prevent or protect against since vendors build products containing components manufactured by subcontractors. It is often difficult to determine the source where different pieces of components are built and installed within the supply chain.

Threat actions include manufacturing faulty or counterfeit parts of components that can be used to disrupt system or network performance, leaving open back doors in hardware that allow attackers easy ways to attack and evade monitoring, as well as easy ways to steal data or tamper with the integrity of existing/new data. Supply Chain attacks may occur during development and production, updates, distribution, shipping, at a warehouse, in storage, during operations, or disposal. For this reason, it is imperative that all components selected for use in CSfC solutions are subject to the applicable Supply Chain Risk Management (SCRM) process to reduce the risk of acquiring compromised components.

Each component that is selected from the CSfC Components List shall go through a Product Supply Chain Threat Assessment to determine the appropriate mitigations for the intended application of the component per the organization's AO/DAA-approved Product Supply Chain Threat Assessment process (See CNSSD 505 Supply Chain Risk Management (SCRM) for additional guidance).

There are doctrinal requirements placed on Product Selection, Implementers, and System Integrators of these solutions to minimize the threat of supply chain attacks.

# 7.9 Integrator Threats

These threats refer to an integrator who has unrestricted access to all components within the solution prior to the customer purchasing and implementing the solution within their system. This is different than a Supply Chain threat in that these integrators have access to all components to be used in the solution, rather than only those being procured from a particular vendor.

Threat actions could include installing or configuring components in a manner that places the organization at risk for attack or open to an unknown vulnerability that may not be detected through normal tests, scans, and security counter-measures.

In order to mitigate this threat, integrators are required to be cleared to the highest level of data protected by the Campus WLAN solution. To further reduce the integrator threat, a customer may wish to use multiple integrators, such that no one integrator has access to all components of the solution.

#### 8 INFORMATION TO SUPPORT AUTHORIZING OFFICIAL

This section details items that likely will be necessary for the implementing organization to obtain approval from the system AO. The implementing organization and AO have obligations to perform the following:

- The implementing organization, possibly with support from a System Integrator, instantiates a solution implementation that follows the NSA-approved Capability Package.
- The implementing organization has a testing team develop a Test Plan and perform testing of the Campus IEEE 802.11 WLAN Architecture solution, see Section 12.
- The implementing organization has system certification and accreditation performed utilizing the risk assessment information referenced in Section 9.
- The implementing organization provides the results from system certification and accreditation to the AO for use in making an approval decision.
- The implementing organization registers the solution with NSA and registers again yearly to validate its continued use. The validation should include a review of the latest version of the Capability Package and associated Risk Assessment.

The system AO maintains configuration control of the approved solution implementation over the lifecycle of the solution. Additionally, the AO should ensure that the solution remains properly configured, with all required security updates installed.

To comply with this Capability Package, the AO must thoroughly review the risk assessment and determine that the residual risks are acceptable for the system implementing the solution. It is strongly recommended that others associated with integrating, administering, and auditing the system also review the risk assessment. The classified risk assessment document for the WLAN Architecture can be obtained by contacting the NSA/IAD Client Advocate for the implementing organization. The classified risk assessment document for the Campus IEEE 802.11 WLAN Solution is also available on the SIPRNet CSfC website.

#### 9 RISK ASSESSMENT

The risk assessment of the Campus WLAN solution presented in this Capability Package focuses on the types of attacks that are feasible against this solution and the mitigations that can be employed. Customers should contact their NSA/IAD Client Advocate to request this document, or visit the SIPRNet CSfC site for information. The process for obtaining the risk assessment is available on the SIPRNet CSfC website. The AO/DAA shall be provided a copy of the NSA risk assessment for their consideration in approving the use of the solution.

# **10 CAMPUS WLAN SOLUTION REQUIREMENTS**

Capability Packages provide architecture and configuration information that allow customers to select COTS products from CSfC component lists for their solution and then to properly configure those products to achieve a level of assurance sufficient for protecting classified data. CSfC component lists consist of eligible COTS products identified by model/version numbers that have met appropriate Protection Profile requirements.

This section contains requirements applicable to the Campus WLAN solution components. In this section, a series of overarching architectural requirements are given for maximizing the independence between the components within the solution. This independence will increase the level of effort required to compromise this solution.

The products that are approved for use in this solution will be listed on the CSfC Components List on the IAD/CSfC website (http://nsagov.nsa.gov/ia/programs/csfc\_program/index.shtml). No single commercial product shall be used to protect classified information. The only approved methods for using COTS products to protect classified information in transit on a Campus WLAN follow the requirements outlined in this Capability Package.

Once the products for the solution are selected, each product shall go through a Product Supply Chain Threat Assessment to determine the appropriate mitigations for the intended application of the component per the organization's DAA/AO approved Product Supply Chain Threat Assessment process. (See CNSSD 505 Supply Chain Risk Management (SCRM) for additional guidance.)

The Capability Package includes two categories of requirements specified based on the below guidance:

- An Objective (O) requirement specifies a feature or function that is desired or expected.
   Organizations should implement objective requirements in lieu of the corresponding Threshold requirement where feasible.
- A Threshold (T) requirement specifies a minimum acceptable feature or function that still
  provides the needed capabilities if the corresponding objective requirement cannot reasonably
  be met (e.g., due to system maturity). A solution implementation must satisfy all applicable
  Threshold requirements, or their corresponding Objective requirements, in order to comply with
  this Capability Package.

In many cases, the Threshold requirement also serves as the Objective requirement (T=O). Where both a Threshold requirement and a related Objective requirement exist, the Objective requirement improves upon the Threshold requirement and may replace the Threshold requirement in future versions of this Capability Package.

In order to comply with this Capability Package, a solution must at minimum implement all Threshold requirements associated with each of the architectures it supports, and should implement the Objective requirements associated with those architectures where feasible.

# **10.1 CSfC Overall Solution Requirements**

**Table 1 CSfC Overall Solution Requirements** 

| Req#      | Requirement Description   | Threshold/<br>Objective |
|-----------|---|-------------------------|
| WLAN-SR-1 | Default accounts, passwords, community strings, and other default access control mechanisms for all components shall be changed or removed.   | T=O                     |
| WLAN-SR-2 | The Gray management network traffic shall be physically or cryptographically separate from the data traffic on the Gray network.  | T=O                     |
| WLAN-SR-3 | The default, self-signed or proprietary device certificates, which are frequently preinstalled by the vendor, on all components shall be removed, except for those necessary for installing vendor updates. | 0                       |

| Req #     | Requirement Description  | Threshold/<br>Objective |
|-----------|--|-------------------------|
| WLAN-SR-4 | Any built-in, pre-loaded, or previously trusted loaded CA records, except those necessary for updates by the vendors, shall be deleted from each component before introducing it to the architecture.  | 0                       |
| WLAN-SR-5 | The time of day on the Inner VPN Gateways and each component within the Red network shall be synchronized with the same time source located in the Red network.  | T=O                     |
| WLAN-SR-6 | The time of day on the WLAN Authentication Server, WLAN Controller, and each component within the Gray network shall be synchronized with the same time source located in the Gray Management network. | T=0                     |
| WLAN-SR-7 | All components shall be properly configured according to local policy and U.S. Government guidance (e.g., DISA gold disk, NSA guidelines).   | T=O                     |
| WLAN-SR-9 | All components shall be configured to protect the confidentiality and integrity of stored private keys using an auxiliary password of configurable length and complexity.                              | 0                       |

# **10.2 CSfC Product Selection Requirements**

# **Table 2 Product Selection Campus WLAN Architecture Requirements**

| Req#      | Requirement Description   | Threshold/<br>Objective |
|-----------|---|-------------------------|
| WLAN-PS-1 | <ul> <li>The Wireless System and VPN Gateways shall either:</li> <li>come from different manufacturers, where neither manufacturer is a subsidiary of the other; or</li> <li>be two different products from the same manufacturer, where NSA has determined that the two products meet the CSfC Program's criteria for implementation independence.</li> </ul>            | T=O                     |
| WLAN-PS-2 | <ul> <li>The WLAN Authentication Server and VPN Gateways shall either:</li> <li>come from different manufacturers, where neither manufacturer is a subsidiary of the other; or</li> <li>be two different products from the same manufacturer, where NSA has determined that the two products meet the CSfC Program's criteria for implementation independence.</li> </ul> | T=O                     |
| WLAN-PS-3 | <ul> <li>The WLAN Client and VPN Client shall either:</li> <li>come from different manufacturers, where neither manufacturer is a subsidiary of the other; or</li> <li>be two different products from the same manufacturer, where NSA has determined that the two products meet the CSfC Program's criteria for implementation independence.</li> </ul>                  | T=O                     |
| WLAN-PS-4 | <ul> <li>The WLAN Authentication Server and VPN Client shall either:</li> <li>come from different manufacturers, where neither manufacturer is a subsidiary of the other; or</li> <li>be two different products from the same manufacturer, where NSA has determined that the two products meet the CSfC Program's criteria for implementation independence.</li> </ul>   | T=O                     |

| Req#       | Requirement Description  | Threshold/<br>Objective |
|------------|--|-------------------------|
| WLAN-PS-5  | <ul> <li>The Wireless System and VPN Client shall either:</li> <li>come from different manufacturers, where neither manufacturer is a subsidiary of the other; or</li> <li>be two different products from the same manufacturer, where NSA has determined that the two products meet the CSfC Program's criteria for implementation independence.</li> </ul>                         | T=O                     |
| WLAN-PS-6  | <ul> <li>The VPN Gateway and WLAN Client shall either:</li> <li>come from different manufacturers, where neither manufacturer is a subsidiary of the other; or</li> <li>be two different products from the same manufacturer, where NSA has determined that the two products meet the CSfC Program's criteria for implementation independence.</li> </ul>                            | T=O                     |
| WLAN-PS-7  | <ul> <li>The WLAN CA and VPN CAs shall either:</li> <li>come from different manufacturers, where neither manufacturer is a subsidiary of the other; or</li> <li>be two different products from the same manufacturer, where NSA has determined that the two products meet the CSfC Program's criteria for implementation independence.</li> </ul>                                    | 0                       |
| WLAN-PS-8  | The Wireless System, WLAN Authentication Server, and the VPN Gateway shall be logically separated using a NSA-approved mechanism.  | Т                       |
| WLAN-PS-9  | The Wireless System, WLAN Authentication Server, and the VPN Gateway shall be run on physically separate hardware.   | 0                       |
| WLAN-PS-10 | On the EUD, the VPN client and the WLAN client applications shall run on different OS's. Differences between Service Packs (SP) or version numbers for a particular vendor's OS do not provide adequate diversity.   | 0                       |
| WLAN-PS-11 | The WLAN Controller and the VPN Gateway shall not utilize the same OS for critical IA security functionality. Differences between Service Packs (SP) and version numbers for a particular vendor's OS do not provide adequate diversity.   | T=O                     |
| WLAN-PS-12 | The products selected for the Campus WLAN solution shall be from the CSfC Component List.  | T=0                     |
| WLAN-PS-13 | Each component that is selected out of the CSfC Components List shall go through a Product Supply Chain Threat Assessment to determine the appropriate mitigations for the intended application of the component per the organization's DAA/AO approved Product Supply Chain Threat Assessment process. (See CNSSD 505 Supply Chain Risk Management (SCRM) for additional guidance.) | T=O                     |
| WLAN-PS-14 | The cryptographic libraries used by the Wireless System and VPN Gateway shall be different independent implementations from different vendors.   | T=O                     |
| WLAN-PS-15 | The cryptographic libraries used by the WLAN Client and VPN Client and shall be different independent implementations from different vendors.  | T=O                     |
| WLAN-PS-16 | The cryptographic libraries used by the WLAN CA and VPN CA and shall be different independent implementations from different vendors.  | 0                       |

**Table 3 WLAN Solution Component Selection Restrictions** 

| T (Threshold) or O (Objective) = indicates that the two components cannot originate from the same manufacturer. | VPN Client | WLAN Client | VPN Gateway | Wireless System | WLAN Authentication Server | WLAN CA | VPN CA |
|---|------------|-------------|-------------|-----------------|----------------------------|---------|--------|
| VPN Client  |            | T=O         |             | T=O             | T=O                        |         |        |
| WLAN Client   | T=O        |             | T=O         |                 |                            |         |        |
| VPN Gateway   |            | T=O         |             | T=O             | T=O                        |         |        |
| Wireless System   | T=O        |             | T=O         |                 |                            |         |        |
| WLAN Authentication Server  | T=O        |             | T=O         |                 |                            |         |        |
| WLAN CA   |            |             |             |                 |                            |         | 0      |
| VPN CA  |            |             |             |                 |                            | 0       |        |

Table 4 Applicable CSfC Component Lists for the Campus WLAN Solution

| Component                  | CSfC Component List   |
|----------------------------|---|
| Wireless System            | WLAN Access System  |
| WLAN Client                | WLAN Client   |
| WLAN Certificate Authority | Certificate Authority or Enterprise CA located in Gray Management network |
| VPN Gateway                | IPsec VPN Gateway   |
| VPN Client                 | IPsec VPN Client  |
| VPN Certificate Authority  | Certificate Authority or Enterprise CA located in Red network             |
| End User Device            | Mobile Device***  |
| WIDS                       | N/A   |

<sup>\*\*\*</sup> The CSfC Components List for Mobile Devices will include EUDs that have passed NIAP's Mobile Device Framework Protection Profile, passed all applicable FIPS requirements, and for which NSA and the mobile device vendor have agreed to a CSfC MoA. Other End User Devices may be used in CSfC WLAN CP solutions; however, the solution accreditor must ensure all such devices comply with the 20 EUD requirements listed below.

# 10.3 Configuration Requirements for the End User Device (EUD)

If the EUD OS provides robust key and certificate storage capabilities, it is acceptable to use the OS key and certificate store for both the WLAN and VPN clients. However, each client must be able to select the

correct private key for authenticating itself and the correct root key certificate for validating certificates received from the WLAN Authentication Server and VPN Gateway. Accordingly, key storage and selection requirements are divided among the WLAN-EUD, WLAN Client WLAN-WC, and VPN Client WLAN-VC sections.

Table 5 WLAN End User Device (EUD) Requirements

| Req #      | Requirement Description   | Threshold/<br>Objective |
|------------|---|-------------------------|
| WLAN-EU-1  | The EUD shall restrict configuration (SSID and authentication mechanism) of authorized WLANs to authorized administrators.  | 0                       |
| WLAN-EU-2  | The EUD shall be configured with separate authentication and privileges for administrative and user roles.  | T=O                     |
| WLAN-EU-3  | The EUD shall be loaded with only approved software.  | 0                       |
| WLAN-EU-4  | The EUD shall restrict installation and removal of software to authorized administrators.   | 0                       |
| WLAN-EU-5  | The EUD shall require a user to log in prior to granting access to any EUD functionality.   | T=O                     |
| WLAN-EU-6  | The EUD shall be configured to limit the number of incorrect logins per a configurable period of time either by erasing the configuration and data stored on the device or by prohibiting login attempts for a configured period of time. | T=O                     |
| WLAN-EU-7  | The EUD shall lock the screen and require user re-authentication after a configurable period of inactivity.   | T=O                     |
| WLAN-EU-8  | The EUD shall display WLAN and VPN secure connection status information.  | T=O                     |
| WLAN-EU-9  | The EUD with the exception of the Wireless Client shall be managed only on the Red network accessible via the Campus WLAN.  | T=O                     |
| WLAN-EU-10 | The EUD shall only be configured to connect to application services on the Red network accessible via the Campus WLAN.  | T=O                     |
| WLAN-EU-11 | The EUD shall be configured such that WLAN and VPN encryption services cannot be bypassed.  | 0                       |
| WLAN-EU-12 | The EUD shall be configured such that WLAN and VPN services cannot be disabled.   | 0                       |
| WLAN-EU-13 | The EUD shall be configured to disable all wireless capabilities except 802.11.   | T=O                     |
| WLAN-EU-14 | The EUD shall either implement an NSA-approved data-at-rest (DAR) solution or prohibit local user storage of information retrieved from the red network.  | 0                       |
| WLAN-EU-15 | The EUD firewall shall be configured to allow only IKE, IPsec, and WPA2 authentication traffic.   | 0                       |
| WLAN-EU-16 | The EUD shall provide a hardware root of trust, trusted boot, and attestation that interoperates with the infrastructure to support remote assessment of integrity and compliance status.   | 0                       |
| WLAN-EU-17 | The EUD shall be configured to use host-based security services (e.g. anti-virus and IDS).  | 0                       |
| WLAN-EU-18 | The EUD shall include tamper detection technology that provides evidence to end-users that unauthorized hardware modifications may have been performed (e.g., tamper seals).  | T=O                     |

| Req#       | Requirement Description   | Threshold/<br>Objective |
|------------|---|-------------------------|
| WLAN-EU-19 | The EUD shall be treated as classified at all times if the device does not have an NSA-approved data-at-rest (DAR) solution | T=O                     |
| WLAN-EU-20 | The EUD shall be re-provisioned if there is any reason to believe it has been compromised.                                  | T=O                     |

# 10.4 Configuration Requirements for the WLAN Client (WC)

# Table 6 WLAN Client (WC) Configuration Requirement

| Req #      | Requirement Description   | Threshold/<br>Objective |
|------------|---|-------------------------|
| WLAN-WC-1  | The WLAN Client tunnel shall be established at EUD start-up.  | 0                       |
| WLAN-WC-2  | The WLAN Client shall authenticate the identity of the WLAN Authentication Server by verifying that the WLAN Authentication Server's certificate chain is rooted by the WLAN trusted root Certificate Authority.  | T=0                     |
| WLAN-WC-3  | The WLAN Client shall be configured to authenticate only specific servers through setting the client to accept only a WLAN Authentication Server certificate that contains a particular Distinguished Name or Subject Alternate Name (i.e., the client looks for the specified server name in the certificate during verification). | 0                       |
| WLAN-WC-4  | A unique device certificate shall be loaded into the WLAN Client along with the corresponding CA (signing) certificate.   | T=O                     |
| WLAN-WC-5  | The device certificate shall be used for WLAN Client authentication during EAP-TLS.   | T=O                     |
| WLAN-WC-6  | The WLAN Client shall provide the user with advance warning that the WLAN Client's device certificate is due to expire.   | 0                       |
| WLAN-WC-7  | The WLAN Client shall negotiate new session keys with the Wireless System at least once per hour.   | 0                       |
| WLAN-WC-8  | The WLAN Client shall be prevented from using ad hoc mode (client-to-client connections).   | T=O                     |
| WLAN-WC-9  | The WLAN Client shall be prevented from using network bridging.   | T=O                     |
| WLAN-WC-10 | The WLAN Client shall only associate with authorized SSIDs.   | 0                       |
| WLAN-WC-11 | The WLAN Client shall verify that the WLAN Authentication Server X.509v3 certificate contains the TLS Web Server Authentication Object Identifier (id-kp-serverAuth 1.3.6.1.5.5.7.3.1) in the Extended Key Usage extension.   | T=0                     |
| WLAN-WC-12 | The device certificate for the WLAN Client shall contain an extendedKeyUsage field indicating support for Client Authentication (Object Identifier (OID) 1.3.6.1.5.5.7.3.2).  | T=O                     |
| WLAN-WC-13 | The WLAN Client shall be managed only on the Gray Management Network accessible via the Campus WLAN.  | T=O                     |

# **Table 7 Wireless Link Requirements**

| Req #     | Requirement Description  | Threshold/<br>Objective |
|-----------|--|-------------------------|
| WLAN-WL-1 | Prior to 1 October 2015, the WLAN Client and the Wireless System shall use protocols and algorithms selected from Table A-8 that are approved to protect the highest classification level of the Red Network data. | T                       |
| WLAN-WL-2 | Prior to 1 October 2015, the WLAN Client and the Wireless System shall use protocols and algorithms selected from Table A-9 that are approved to protect the highest classification level of the Red Network data. | 0                       |
| WLAN-WL-3 | After 1 October 2015, the WLAN Client and the Wireless System shall use protocols and algorithms selected from Table A-9 that are approved to protect the highest classification level of the Red Network data.    | Т                       |
| WLAN-WL-4 | The WLAN Client and the Wireless System shall use protocols and algorithms selected from the Algorithm Suite for TS and Below in Table A-9.  | 0                       |
| WLAN-WL-5 | The WLAN Client and the Wireless System shall operate in WPA2-<br>Enterprise mode.   | T=O                     |
| WLAN-WL-6 | The WLAN Client and the Wireless System shall use Group Temporal Key (GTK) key encryption that implements NIST AES Key Wrap with HMAC-SHA1-128 as specified in Section 11 of IEEE 802.11-2012.                     | T=0                     |
| WLAN-WL-7 | The WLAN Client and the Wireless System shall use integrity algorithms that implements NIST AES Key Wrap with HMAC-SHA1-128 as specified in Section 11 of IEEE 802.11-2012.  | T=O                     |

# **Table 8 Approved Interim Algorithms**

| Security Service                      | Algorithm Suite<br>(for TS and below)  | Algorithm Suite<br>(for S and below)                    | Specifications                                    |
|---------------------------------------|--|---|---|
| Confidentiality (Encryption)          | AES with 128 bits for WPA2<br>AES with 256 bits for VPN  | AES with 128 bits                                       | FIPS PUB 197                                      |
| Authentication<br>(Digital Signature) | WLAN Client: RSA (2048 bit<br>modulus) with SHA-384<br>WLAN Authentication<br>Server: ECDSA over the<br>curve P-384 with SHA-384 | RSA (2048 bit modulus) with<br>SHA-1                    | FIPS PUB 186-3                                    |
| Key Exchange/<br>Establishment        | Ephemeral ECDH over the curve P-384 (DH Group 20)  | Ephemeral 2048-bit Modular Exponentiation (DH Group 14) | NISP SP 800-56A<br>IETF RFC 6379<br>IETF RFC 3526 |
| Integrity (Hashing)                   | SHA-1  | SHA-1   | FIPS PUB 180-4                                    |

**Table 9 Approved Suite B Algorithms** 

| Security Service                   | Algorithm Suite<br>(for TS and below)             | Algorithm Suite<br>(for S and below)              | Specification   |
|------------------------------------|---|---|---|
| Confidentiality (Encryption)       | AES with 256 bits                                 | AES with 128 bits                                 | FIPS PUB 197  |
| Authentication (Digital Signature) | ECDSA over the curve P-<br>384 with SHA-384       | ECDSA over the curve P-<br>256 with SHA-256       | FIPS PUB 186-3  |
| Key Exchange/<br>Establishment     | Ephemeral ECDH over the curve P-384 (DH Group 20) | Ephemeral ECDH over the curve P-256 (DH Group 19) | NIST SP 800-56A<br>IETF RFC 6379 Suite<br>B Cryptographic<br>Suites for IPsec |
| Integrity (Hashing)                | SHA-384   | SHA-256   | FIPS PUB 180-4  |

# 10.5 Configuration Requirements for the VPN Client (VC)

# **Table 10 VPN Client (VC) Configuration Requirements**

| Req#      | Requirement Description  | Threshold/<br>Objective |
|-----------|--|-------------------------|
| WLAN-VC-1 | Each VPN Client shall be configured with a unique private key and corresponding X.509 version 3 certificate. | T=O                     |
| WLAN-VC-2 | Each VPN Client shall use the unique private key for authenticating to the VPN Gateway.                      | T=O                     |
| WLAN-VC-3 | The VPN Client shall provide the user with advance warning that the VPN client certificate is due to expire. | 0                       |
| WLAN-VC-4 | The VPN Client shall be configured to prohibit split tunneling.  | T=O                     |

# 10.6 Configuration Requirements for Both VPN Components (CR)

# **Table 11 Configuration Requirements for Both VPN Components**

| Req #     | Requirement Description  | Threshold/<br>Objective |
|-----------|--|-------------------------|
| WLAN-CR-1 | Prior to 1 October 2015, the VPN Components shall use protocols and algorithms for creating all VPN tunnels selected from an Algorithm Suite in Table A-8 that are approved to protect the highest classification level of the Red Network data (or meet WLAN-CR-2). | Т                       |
| WLAN-CR-2 | Prior to 1 October 2015, the VPN Components shall use protocols and algorithms for creating all VPN tunnels selected from an Algorithm Suite in Table A-9 that are approved to protect the highest classification level of the Red Network data.                     | 0                       |
| WLAN-CR-3 | After 1 October 2015, the VPN Components shall use protocols and algorithms for creating all VPN tunnels selected from an Algorithm Suite in Table A-9 that are approved to protect the highest classification level of the Red Network data.                        | Т                       |
| WLAN-CR-4 | VPN Components shall use protocols and algorithms selected from the Algorithm Suite for TS and Below in Table A-9 (or meet WLAN-CR-4).   | 0                       |

| WLAN-CR-5  | All VPN Components shall only offer algorithms identified in WLAN-CR-1 thru WLAN-CR-4.   | T=O |
|------------|--|-----|
| WLAN-CR-6  | VPN Components shall use IKEv1 (RFC 2409) for key exchange in Main Mode on Phase 1 (or meet WLAN-CR-7).  | Т   |
| WLAN-CR-7  | VPN Components shall use IKEv2 (RFC 5996) for key exchange.  | 0   |
| WLAN-CR-8  | The IPsec tunnel between the VPN Client and the VPN Gateway shall use AES Cipher Block Chaining mode for IKE encryption.   | T=O |
|            |  |     |
| WLAN-CR-11 | VPN Components shall use Galois Counter Mode (GCM) for ESP Encryption.   | T=O |
| WLAN-CR-12 | VPN Components shall set ESP SA lifetime to 8 hours or less.   | T=O |
| WLAN-CR-13 | VPN Components shall set IKE SA lifetime to 24 hours.  | T=O |
| WLAN-CR-14 | VPN Components shall use protocols and algorithms for creating all VPN tunnels selected from an Algorithm Suite 2 in Table A-9.  | 0   |
| WLAN-CR-15 | The packet size for packets leaving the external interface of the Inner VPN component shall be configured to keep the packets from being fragmented and impacting performance. This requires proper configuration of the Maximum Transmission Unit (MTU) (for IPv4) or Path MTU (PMTU) (for IPv6) and should consider the Black network and Outer component MTU/PMTU values to achieve this. | 0   |
| WLAN-CR-16 | For solutions using IPv4, the external interface of each VPN component shall drop all packets that use IP options (e.g., if the first byte is not 0x45, then the packet shall be dropped). A similar requirement is not placed on IPv6 instantiations.   | T=O |
| WLAN-CR-17 | Device certificates shall be used for VPN Gateway and VPN Client authentication during IKE.  | T=O |
| WLAN-CR-18 | The VPN Client and the VPN Gateway shall be configured to accept only certificates that have been signed by the VPN trusted root Certificate Authority for the VPN layer of the Campus WLAN Solution.  | T=O |
| WLAN-CR-19 | The VPN Client and the VPN Gateway shall validate certificate signatures and verify connection authorization based on the be Distinguished Name or Subject Alternate Name included in the certificate received from the opposite end of the VPN connection.  | 0   |

# 10.7 Configuration Requirements for the WLAN System (WS)

The Wireless System is involved in establishing two encrypted channels. The first is a point-to-point IPsec tunnel-mode association with the WLAN Authentication Server for securely passing RADIUS attributes and the PMK. Once WLAN Authentication Server passes the PMK to the Wireless System, the Wireless System establishes an encrypted channel with the WLAN Client for passing data. The Wireless System acts as a pass-through for the initial authentication exchange between the WLAN Client and the WLAN Authentication Server during which the PMK is securely negotiated.

# 10.7.1 Wireless System Physical Configuration

# **Table 12 Wireless System Configuration Requirements**

| Req#      | Requirement Description   | Threshold/<br>Objective |
|-----------|---|-------------------------|
| WLAN-WS-1 | The Wireless System shall not operate in the same spaces as a non U.S. government controlled unclassified WLAN.   | 0                       |
| WLAN-WS-2 | The Wireless System shall act as an EAP-TLS pass-through between the WLAN Client and WLAN Authentication Server for authentication and key establishment. | T=O                     |
| WLAN-WS-3 | The Wireless System shall negotiate new session keys with the WLAN Clients at least once per hour.  | T=O                     |
| WLAN-WS-4 | The Wireless System shall be dedicated to a single classification level.  | T=O                     |
| WLAN-WS-5 | A unique device certificate shall be loaded into the Wireless System along with the corresponding CA (signing) certificate.                               | 0                       |

# 10.7.2 Wireless Infrastructure Authentication

# **Table 13 Wireless Infrastructure Authentication Requirements**

| Req#       | Requirement Description  | Threshold/<br>Objective |
|------------|--|-------------------------|
| WLAN-IA-1  | Communications between the Wireless System and the WLAN Authentication Server shall use the RADIUS protocol encrypted using point-to-point tunnel-mode IPsec.  | T=O                     |
| WLAN-IA-2  | The IPsec tunnel between the Wireless System and the WLAN Authentication Server shall use IKEv1 (RFC 2409) key exchange in Main Mode on Phase 1 (or meet WLAN-IA-3).   | Т                       |
| WLAN-IA-3  | The IPsec tunnel between the Wireless System and the WLAN Authentication Server shall use IKEv2 (RFC 5996) key exchange.   | 0                       |
| WLAN-IA-4  | The IKE exchange between the Wireless System and the WLAN Authentication Server shall use DH Group 14 (or meet WLAN-IA-8).   | Т                       |
| WLAN-IA-5  | The IKE exchange between the Wireless System and the WLAN Authentication Server shall use SHA-1 for integrity (or meet WLAN-IA-8).   | Т                       |
| WLAN-IA-6  | The ESP security association between the Wireless System and the WLAN Authentication Server shall use SHA-1 for integrity (or meet WLAN-IA-8).   | Т                       |
| WLAN-IA-7  | After 1 October 2015, the IKE exchange and IPsec tunnel between the Wireless System and the WLAN Authentication Server shall use protocols and algorithms selected from Table A-9 that are approved to protect the highest classification level of the Red Network data. | T                       |
| WLAN-IA-8  | The IKE exchange and IPsec tunnel between the Wireless System and the WLAN Authentication Server shall use protocols and algorithms selected from the Algorithm Suite for TS and Below in Table A-9.   | 0                       |
| WLAN-IA-10 | The ESP SA tunnel between the Wireless System and the WLAN Authentication Server shall be ESP using AES in Cipher Block Chaining (CBC) mode with a SHA-based HMAC for integrity (or meet WLAN-IA-11).  | Т                       |

| WLAN-IA-11 | The ESP SA tunnel between the Wireless System and the WLAN Authentication Server shall be ESP use AES in Galois Counter Mode (GCM) mode.   | 0   |
|------------|--|-----|
| WLAN-IA-12 | The lifetime of the IKE SA between the Wireless System and the WLAN Authentication Server shall be set to 24 hours.  | T=O |
| WLAN-IA-13 | The lifetime of the ESP SA between the Wireless System and the WLAN Authentication Server shall be set to 8 hours or less.   | T=O |
| WLAN-IA-14 | The Wireless System and the WLAN Authentication Server shall authenticate one another using pre-shared keys (or meet WLAN-IA-15).  | Т   |
| WLAN-IA-15 | The Wireless System and the WLAN Authentication Server shall authenticate one another using X.509 version 3 certificates.  | 0   |
| WLAN-IA-16 | Composition rules for a pre-shared key between the Wireless System and the WLAN Authentication Server shall be set by the Security Administrator. This requirement is N/A if WLAN-IA-15 is met.  | Т   |
| WLAN-IA-17 | The estimated entropy of a pre-shared key between the Wireless System and the WLAN Authentication Server shall be a minimum of 256 bits (for Top Secret and below) or 128 bits (for Secret and below). This requirement is N/A if WLAN-IA-15 is met. | Т   |
|            |  |     |
| WLAN-IA-19 | The IKE exchange between the Wireless System and the WLAN Authentication Server shall use DH Group 19 and/or 20.   | 0   |

# **10.7.3** Wireless Authentication and Authorization Requirements

**Table 14 Wireless Authentication and Authorization Requirements** 

| Req #     | Requirement Description   | Threshold/<br>Objective |
|-----------|---|-------------------------|
| WLAN-AA-1 | The WLAN Authentication Server and WLAN Client shall perform mutual authentication using EAP-TLS.               | T=O                     |
| WLAN-AA-2 | The WLAN Client and the WLAN Authentication Server shall use AES in CBC during mode in the EAP TLS negotiation. | T=O                     |

# 10.7.4 Wireless Authentication Server to WLAN Client Requirements Table 15 Wireless Authentication Server to WLAN Client Requirements

| Req#      | Requirement Description  | Threshold/<br>Objective |
|-----------|--|-------------------------|
| WLAN-WA-1 | The WLAN Authentication Server shall disallow any authentication methods other than EAP-TLS.   | T=O                     |
| WLAN-WA-2 | A unique device certificate shall be loaded into the WLAN Authentication Server along with the corresponding CA (signing) certificate.   | T=O                     |
| WLAN-WA-3 | The WLAN Authentication Server shall check that the WLAN Client's certificate is authorized, which can include a check against a Certificate Revocation List (CRL) or a whitelist. | T=O                     |

| WLAN-WA-4 | The WLAN Authentication Server shall receive a current CRL either by retrieving it from an authoritative source or by the Security Administrator installing an updated CRL before the previous CRL expires.                 | T=0 |
|-----------|---|-----|
| WLAN-WA-5 | The device certificate for the WLAN Authentication Server shall contain an extendedKeyUsage field indicating support for Server Authentication (Object Identifier (OID) 1.3.6.1.5.5.7.3.1).                                 | T=O |
| WLAN-WA-6 | The WLAN Authentication Server shall only successfully authenticate a WLAN Client if the WLAN Client's certificate contains an extendedKeyUsage field indicating support for Client Authentication (OID 1.3.6.1.5.5.7.3.2). | T=O |
| WLAN-WA-7 | The WLAN Authentication Server shall authenticate the identity of the WLAN Client by verifying that the Distinguished Name or the Subject Alternate Name contained in the WLAN Client's certificate appears on a whitelist. | T=0 |
| WLAN-WA-8 | The device certificate shall be used for Wireless Authentication Server authentication during EAP-TLS.  | T=O |
| WLAN-WA-9 | The WLAN Authentication Server shall authenticate the identity of the WLAN Client by verifying that the WLAN Client's certificate chain is rooted by the WLAN trusted root Certificate Authority.                           | T=0 |

# **10.8 Port Filtering Requirements**

Port Filtering is composed of a component configured with access control lists (ACLs). The system ensures that the traffic flowing to and from each component on the network is appropriate for the functionality of the component within the Campus WLAN solution.

**Table 16 Port Filtering (PF) Requirements** 

| Req#      | Requirement Description   | Threshold/<br>Objective |
|-----------|---|-------------------------|
| WLAN-PF-1 | For all interfaces connected to Black network, traffic filtering rules shall be applied to both inbound and outbound traffic, such that only WPA2 (as defined in this Capability Package) approved by policy are allowed. All packets not explicitly allowed shall be blocked.  | T=O                     |
| WLAN-PF-2 | For all interfaces connected to a Gray network, traffic filtering rules shall be applied to both inbound and outbound traffic, such that only EAP-TLS, IKE, IPsec, and control plane protocols (as defined in this Capability Package) approved by policy are allowed. All packets not explicitly allowed shall be blocked. | T=O                     |
| WLAN-PF-3 | Traffic filtering rules on the VPN Gateway shall be applied based on known addresses or address ranges assigned to EUDs to further protect against unknown IPsec traffic.   | 0                       |
| WLAN-PF-4 | Traffic filtering rules on the EUD shall be applied based on known VPN Gateway addresses or address range to further protect against unknown IPsec traffic.   | T=O                     |
| WLAN-PF-5 | Any service or feature that allows the EUD to contact a third party server (such as one maintained by the manufacturer) shall be blocked.   | T                       |
| WLAN-PF-6 | Any service or feature that allows the EUD to contact a third party server (such as one maintained by the manufacturer) shall be disabled.  | 0                       |

| WLAN-PF-7 | The Wireless System shall block all data (ports and IP addresses) on their Gray Management network interface that is not necessary for the management of the Wireless System. | T=O |
|-----------|---|-----|
| WLAN-PF-8 | Traffic filtering rules on all Black network interfaces of the Wireless System shall be based on known MAC addresses of EUDs to further protect against unknown WLAN Clients. | T=O |
| WLAN-PF-9 | Traffic filtering rules on the EUD shall be applied based on known VPN Gateway addresses or address range to further protect against unknown IPsec traffic.                   | T=O |

# 10.9 Configuration of the VPN Gateway (VG)

# **Table 17 VPN Gateway (VG) Requirements**

| Req#      | Requirement Description  | Threshold/<br>Objective |
|-----------|--|-------------------------|
| WLAN-VG-1 | A unique device certificate shall be loaded onto each VPN Gateway along with the corresponding CA (signing) certificate.   | T=O                     |
| WLAN-VG-2 | The private key stored on VPN Gateway shall not be accessible through any interface.   | T=O                     |
| WLAN-VG-3 | The VPN Gateway shall be configured to prohibit split tunneling  | T=O                     |
| WLAN-VG-4 | VPN Gateway authentication shall include a check that the certificate is authorized which can include a Certificate Revocation List (CRL) or whitelist.                                | T=O                     |
| WLAN-VG-5 | The VPN Gateway authentication shall include a validation check on the Distinguished Name or Subject Alternate Name in the VPN Client's X.509v3 device certificate against a database. | T=0                     |
| WLAN-VG-6 | The VPN Gateway authentication shall include a check that the certificate is not expired.  | T=O                     |

# 10.10 Configuration Requirements for Wireless Intrusion Detection System (WIDS)

# **Table 18 Wireless IDS (WIDS) Configuration Requirements**

| Req#      | Requirement Description  | Threshold/<br>Objective |
|-----------|--|-------------------------|
| WLAN-WI-1 | The WIDS shall be configured with a whitelist of all authorized wireless network devices. (i.e. Access points and EUDs)          | T=O                     |
| WLAN-WI-2 | The WIDS security policy shall be configured to detect use of unauthorized wireless channels by whitelisted devices              | T=O                     |
| WLAN-WI-3 | The WIDS security policy shall be configured to detect whitelisted devices violating SSID cloaking policy                        | T=O                     |
| WLAN-WI-4 | The WIDS security policy shall be configured to detect whitelisted devices violating null SSID association policy                | T=O                     |
| WLAN-WI-5 | The WIDS security policy shall be configured to detect whitelisted devices attempting to use unauthorized authentication methods | T=O                     |
| WLAN-WI-6 | The WIDS security policy shall be configured to detect whitelisted devices attempting to use unauthorized encryption schemes     | T=O                     |

| Req#       | Requirement Description  | Threshold/<br>Objective |
|------------|--|-------------------------|
| WLAN-WI-7  | The WIDS security policy shall be configured to detect whitelisted devices establishing ad hoc connections   | T=O                     |
| WLAN-WI-9  | The WIDS security policy shall be configured to detect EUDs which are not on the whitelist, but are within the coverage area of the authorized Access Points | T=O                     |
| WLAN-WI-10 | The WIDS shall be configured to detect all frames between unauthorized EUDs and authorized access points   | T=O                     |
| WLAN-WI-11 | The WIDS security policy shall be configured to detect simultaneous connections by the same EUD in different physical locations                              | T=O                     |
| WLAN-WI-12 | The WIDS sensors shall not transmit wirelessly   | T=O                     |
| WLAN-WI-13 | The WIDS shall utilize FIPS certified Suite B encryption between all WIDS components   | 0                       |
| WLAN-WI-14 | The WIDS shall utilize two-way authentication between all WIDS components  | 0                       |
| WLAN-WI-15 | The WIDS shall capture and parse all IEEE 802.11 traffic up to the maximum bit rate of the wireless access points without dropping frames                    | T=O                     |
| WLAN-WI-16 | The WIDS shall sniff traffic from all IEEE 802.11 channels within the 2.4Ghz, 3.6Ghz, 4.9/5.0Ghz bands   | 0                       |
| WLAN-WI-17 | The WIDS security policy shall be configured to detect any transmission from any other WIDS sensor within range  | T=O                     |
| WLAN-WI-18 | The WIDS shall be configured to geographically locate all IEEE 802.11 wireless hardware operating in the coverage area of the authorized Access Points.      | 0                       |
| WLAN-WI-19 | WIDS security policy shall be configured to log the signal strength of hardware operating in the coverage area of the authorized Access Points.              | T=O                     |
| WLAN-WI-20 | The WIDS shall detect and log when it receives an IEEE 802.11 frame at a signal level substantially above the IEEE standard.                                 | T=O                     |
| WLAN-WI-21 | The WIDS security policy shall be configured to detect RF-based denial-of-service attacks (DoS)  | T=O                     |
| WLAN-WI-22 | The WIDS security policy shall be configured to detect and log all violations of WLAN standards, including, but not limited to, IEEE 802.11 and IEEE 802.1X. | T=O                     |
| WLAN-WI-23 | The WIDS shall perform stateful frame inspection to detect and log attacks spanning multiple frames.   | T=O                     |
| WLAN-WI-24 | The WIDS shall detect and log active probing   | T=O                     |
| WLAN-WI-25 | The WIDS shall detect and log active de-authentication flooding  | T=O                     |
| WLAN-WI-26 | The WIDS shall detect and log disassociation flooding  | T=O                     |
| WLAN-WI-27 | The WIDS shall detect and log RTS/CTS/NAK abuse.   | T=O                     |
| WLAN-WI-28 | The WIDS shall automatically compute a network traffic baseline.   | 0                       |
| WLAN-WI-29 | The Security Administrator shall be able to override the network traffic baseline  | 0                       |
| WLAN-WI-30 | The WIDS shall detect, log, and generate an alarm for deviations from the established network traffic baseline.  | 0                       |

| Req #      | Requirement Description   | Threshold/<br>Objective |
|------------|---|-------------------------|
| WLAN-WI-31 | If the network's activity deviates from a known profile, the WIDS shall use statistical analysis, also known as profile-based or anomaly detection, to generate an alarm.                                   | 0                       |
| WLAN-WI-32 | The WIDS shall monitor bandwidth usage  | T=O                     |
| WLAN-WI-33 | The WIDS shall monitor number of users/wireless clients   | T=O                     |
| WLAN-WI-34 | The WIDS shall monitor times of usage   | T=O                     |
| WLAN-WI-35 | The WIDS shall monitor user/wireless client location  | 0                       |
| WLAN-WI-36 | The WIDS shall monitor type of traffic.   | T=O                     |
| WLAN-WI-37 | The WIDS shall capture a network baseline based on the previous seven days of network traffic for anomaly detection.  | 0                       |
| WLAN-WI-38 | The WIDS shall track the connection status of each client (authorized or unauthorized) in real time including, but not limited to, whether the client is offline, associated, or authentication is pending. | T=O                     |
| WLAN-WI-39 | The WIDS shall detect and log illegal state transitions, such as a client device transmitting data frames to a network device before being associated and authenticated.                                    | T=O                     |
| WLAN-WI-40 | The WIDS shall detect and log any unauthorized IEEE 802.11 transmitters operating in the area detectable by the sensors.  | T=O                     |
| WLAN-WI-41 | The WIDS shall distinguish between the mere existence of unauthorized hardware and an attempt to use that hardware to connect to the wireless network.  | T=O                     |
| WLAN-WI-42 | The WIDS shall detect and log any authorized clients communicating in ad-hoc mode.  | T=O                     |
| WLAN-WI-43 | The WIDS shall detect and log an event where an attacker spoofs the MAC address of an authorized client.  | 0                       |
| WLAN-WI-44 | The WIDS shall detect and log an event where two sensors in physically separate (non-overlapping) locations (such as different buildings) receive frames with the same MAC address at the same time.        | T=0                     |
| WLAN-WI-45 | The WIDS shall detect and log an event where a EUD's MAC address appears in multiple physically distant locations in too short a time span.   | 0                       |
| WLAN-WI-46 | The Security Administrator shall configure the WIDS for the allowable time span where a EUD's MAC address may appear in multiple physically distant locations.  | 0                       |
| WLAN-WI-47 | The WIDS shall detect and log the presence of an IEEE 802.11 bridge   | T=O                     |
| WLAN-WI-48 | The WIDS shall detect and log the presence of a single device transmitting beacons looking for a bridge   | T=O                     |
| WLAN-WI-49 | The WIDS shall detect and log the presence of two or more devices transmitting bridge data frames.  | T=O                     |
| WLAN-WI-50 | The WIDS shall detect and log unauthorized access points broadcasting with the same SSID as whitelisted access points.  | T=O                     |

| Req#       | Requirement Description   | Threshold/<br>Objective |
|------------|---|-------------------------|
| WLAN-WI-51 | The WIDS shall provide the ability to remove or disable all non-secure communications paths for system updates and event monitoring including, but not limited to, HTTP, SNMPv1, File Transfer Protocol (FTP), and Telnet over both wired and wireless transports. The preferred method is to completely remove these capabilities from the system. | T=O                     |
| WLAN-WI-52 | The WIDS shall be configured to send an alert should any component of the solution fail to communicate  | T=O                     |

# 10.11 Configuration Change Detection (CCD) Requirements

# **Table 19 Configuration Change Detection (CCD) Requirements**

| Req#      | Requirement Description  | Threshold/<br>Objective |
|-----------|--|-------------------------|
| WLAN-CM-1 | A baseline configuration for all components shall be maintained by the Security Administrator and be available to the Auditor. | T=O                     |
| WLAN-CM-2 | An automated process shall ensure that configuration changes are logged.   | T=O                     |
| WLAN-CM-3 | Log messages generated for configuration changes shall include the specific changes made to the configuration.                 | T=O                     |
| WLAN-CM-4 | All components shall be configured with a monitoring service that detects all changes to configuration.                        | 0                       |
| WLAN-CM-5 | The cryptographic modules shall be configured to operate in FIPS mode.   | T=O                     |

# **10.12** Requirements for Infrastructure Component Administration (RA)

The requirements in this section apply to management and administration of infrastructure components. There are currently no requirements specified for Mobile Device Management (MDM).

**Table 20 Component Administration (RA) Requirements** 

| Req#      | Requirement Description   | Threshold/<br>Objective |
|-----------|---|-------------------------|
| WLAN-RA-1 | All administration shall be performed through direct physical access or from an Administration Workstation remotely through SSHv2, IPsec, or TLS.   | T=O                     |
| WLAN-RA-2 | If SSHv2 is utilized for remote management of infrastructure components, the protocol shall be implemented as specified in RFCs 4252-4254 and 6239.   | T=O                     |
| WLAN-RA-3 | If IPsec is utilized for remote management of VPN Gateway and other infrastructure components, the protocol shall be implemented as specified in RFCs 2409, 4302, 4303, 4307, 4308, 5996, 6379, and 6380. | T=O                     |

| WLAN-RA-4 | If TLS is utilized for remote management of infrastructure components, the protocol shall be implemented as specified in RFCs 5246 and 6460. | T=O |
|-----------|--|-----|
| WLAN-RA-6 | Antivirus software shall be running on all Administration Workstations.  | T=O |
| WLAN-RA-7 | The WIDS shall encrypt and sign all alerts pushed to a remote system administrator.  | 0   |
| WLAN-RA-8 | System administrators shall authenticate all alerts received by the WIDS.  | 0   |
| WLAN-RA-9 | All components shall be configured to restrict the IP address range for the network administration device to the smallest range possible.    | T=O |

# 10.13 Network Intrusion Detection System (NIDS) Requirements Table 21 Network Intrusion Detection System (NIDS) Requirements

| Req#      | Requirement Description  | Threshold/<br>Objective |
|-----------|--|-------------------------|
| WLAN-NI-1 | A Network-based Intrusion Detection System (NIDS) shall be deployed on the Gray Management Network to monitor traffic arriving from or leaving to the Wireless System. | 0                       |
| WLAN-NI-2 | The NIDS shall report all matches to the attack signatures on the NIDS to both inbound and outbound traffic.   | 0                       |
| WLAN-NI-3 | The NIDS shall be regularly updated with attack signatures in accordance with local policy.  | 0                       |

# 10.14 Requirements for Auditing (AU)

# **Table 22 Auditing (AU) Requirements**

| Req #     | Requirement Description   | Threshold/<br>Objective |
|-----------|---|-------------------------|
| WLAN-AU-1 | All actions performed on the audit log (off-loading, deletion, etc.) shall be logged on a continuous basis.                         | T=O                     |
| WLAN-AU-2 | All actions involving identification and authentication shall be logged on a continuous basis.                                      | T=O                     |
| WLAN-AU-3 | Attempts to perform an unauthorized action (read, write, execute, delete, etc.) on an object shall be logged on a continuous basis. | T=O                     |
| WLAN-AU-4 | All actions performed by a user with super privileges shall be logged on a continuous basis.  | T=O                     |
| WLAN-AU-5 | Any escalation of user privileges shall be logged on a continuous basis.  | T=O                     |
| WLAN-AU-6 | The firewall shall log all packets that are blocked.  | T=O                     |
| WLAN-AU-7 | The set of auditable events specified in the CPS shall be monitored and logged within the CAs on a continuous basis when in use.    | T=O                     |
| WLAN-AU-8 | Each audit event entry shall record the date and time of the event and identify the time zone offset.                               | T=O                     |
| WLAN-AU-9 | Each audit event entry shall include the identifier of the event.   | T=O                     |

| WLAN-AU-10 | Each audit event entry shall record the type of event.  | T=O |
|------------|---|-----|
| WLAN-AU-11 | Each audit event entry shall record the success or failure of the event to include failure code, when available.  | T=O |
| WLAN-AU-12 | Each audit event entry shall record the subject identity.   | T=O |
| WLAN-AU-13 | Each audit event entry shall record the source address for network based events.  | T=O |
| WLAN-AU-14 | Upon notification of two or more simultaneous connections established by the same device certificate, the Certificate Authority Administrator shall revoke the device certificate and provide an updated Certificate Revocation List (CRL) to the Security Administrator. | T=O |
| WLAN-AU-15 | The Security Administrator shall immediately drop the session upon notification of two or more simultaneous connections established by the same device certificate.   | T=O |
| WLAN-AU-16 | Logs shall be monitored by the Auditor on at least a weekly basis.  | T=O |
| WLAN-AU-17 | All built-in self-test results, which may indicate failures in cryptographic functionality, shall be logged on a continuous basis.  | T=O |
| WLAN-AU-18 | The VPN Gateway shall log when a VPN tunnel is established.   | T=O |
| WLAN-AU-19 | The VPN Gateway shall log when a VPN tunnel is terminated.  | T=O |
| WLAN-AU-20 | The Wireless System shall log when a Client associates to the network.  | T=O |
| WLAN-AU-21 | The Wireless System shall log when a Client dis-associates from the network.  | T=O |
| WLAN-AU-22 | Changes to time shall be logged on a continuous basis.  | T=O |
| WLAN-AU-23 | All event monitoring of the WIDS shall be remotely performed from the Gray Management Network through SSHv2, IPsec, or TLS.   | 0   |
| WLAN-AU-24 | The WIDS shall log when sensors fail to communicate.  | T=O |
| WLAN-AU-25 | The EUD shall audit all successful and unsuccessful logins.   | 0   |
| WLAN-AU-26 | The EUD shall audit all successful and unsuccessful logouts.  | 0   |
| WLAN-AU-27 | The EUD shall audit installation and removal of software.   | 0   |
| WLAN-AU-28 | The EUD shall audit attempts to change security-relevant configuration items.   | 0   |
| WLAN-AU-29 | The EUD shall audit changes to security-relevant configuration items.   | 0   |
| WLAN-AU-30 | The EUD shall audit signature verification and certificate validation.  | 0   |
| WLAN-AU-31 | The EUD shall audit key unlock.   | 0   |
| WLAN-AU-32 | The EUD shall provide a notification if any wireless capability with the exception of Wi-Fi has been enabled by the user.   | 0   |
| WLAN-AU-33 | The EUD shall audit decryption/integrity errors.  | 0   |
| WLAN-AU-34 | Auditors shall detect when two or more simultaneous VPN connections from different IP addresses are established using the same device certificate.  | 0   |

# 10.15 Requirements for Key Management (KM)

# **10.15.1** General Key Management Requirements

# **Table 23 General Key Management Requirements**

| Req#       | Requirement Description   | Threshold/<br>Objective |
|------------|---|-------------------------|
| WLAN-KM-1  | The IPsec VPN and WLAN CAs shall issue X.509 version 3 certificates   | T=O                     |
| WLAN-KM-2  | The CA supporting the IPsec VPN shall be physically separate from the CA supporting the WLAN.   | T=O                     |
| WLAN-KM-3  | The IPsec VPN and WLAN CAs shall each operate under a CPS that is formatted in accordance with Internet Engineering Task Force (IETF) Request for Comments (RFC) 3647.  | T=O                     |
| WLAN-KM-4  | The IPsec VPN and WLAN CAs shall initially key devices within a physical environment accredited to protect the highest classification level of data.  | T=0                     |
| WLAN-KM-5  | The IPsec VPN and WLAN CAs shall rekey infrastructure devices prior to expiration of keys.  | T=O                     |
| WLAN-KM-6  | The certification revocation information of the VPN Gateway and WLAN Authentication Server shall be updated at the same time as the components are rekeyed.   | T=0                     |
| WLAN-KM-7  | If rekeying of the VPN Gateway, WLAN Clients, WLAN Authentication Server, or VPN Clients is not completed prior to expiration of keys, they shall be rekeyed through the same process as initial keying.                        | T=O                     |
| WLAN-KM-8  | Certificate revocation information shall be made available by posting the data to a repository or service that is available for the VPN Gateway and WLAN Authentication Server.   | T=O                     |
| WLAN-KM-9  | New certificates shall be issued as needed in accordance with local policy.   | T=O                     |
| WLAN-KM-10 | CAs shall run anti-virus software.  | T=O                     |
| WLAN-KM-11 | CAs shall not escrow private keys.  | T=O                     |
| WLAN-KM-12 | Locally-run CAs shall have a limited name space to issue certificates.  | T=O                     |
| WLAN-KM-13 | Locally-run CAs shall issue certificates with unique names.   | T=O                     |
| WLAN-KM-14 | The VPN Gateway and WLAN CAs shall generate a unique Distinguished Name (DN) in each certificate issued. (Note that the Common Name is not required to be unique.)  | T=O                     |
| WLAN-KM-15 | Locally-run red network CAs shall assert a registered OID to all of its VPN Components.   | T=O                     |
| WLAN-KM-16 | Enterprise CAs shall assert a registered Object Identifier (OID) to all of its VPN Components.  | 0                       |
| WLAN-KM-17 | Enterprise CAs shall be located on the Red network for Inner VPN Components and on the Gray network for WLAN Components, and be approved to issue certificates (such as one that follows CNSSI 1300 under the NSS PKI Root CA). | T=0                     |
| WLAN-KM-18 | The key validity period for certificates issued by Locally-run CAs shall not exceed 14 months.  | T=0                     |

# **10.15.2** IPsec VPN Key Management Requirements

# **Table 24 IPsec VPN Key Management Requirements**

| Req#       | Requirement Description   | Threshold/<br>Objective |
|------------|---|-------------------------|
| WLAN-KM-19 | The IPsec VPN CA shall use key sizes and algorithms as specified in Table A-8 (or meet WLAN-KM-20).     | Т                       |
| WLAN-KM-20 | The IPsec VPN CA shall use key sizes and algorithms as specified in Table A-9.                          | 0                       |
| WLAN-KM-21 | The IPsec VPN CA shall support key sizes and algorithms as specified in Table A-9 after 1 October 2015. | Т                       |
| WLAN-KM-22 | The WLAN CA shall use key sizes and algorithms as specified in Table A-8 (or meet WLAN-KM-23).          | Т                       |
| WLAN-KM-23 | The WLAN CA shall use key sizes and algorithms as specified in Table A-9.                               | 0                       |
| WLAN-KM-24 | The WLAN CA shall support key sizes and algorithms as specified in Table A-9 after 1 October 2015.      | Т                       |

# **10.15.3** WLAN Key Management Requirements

# **Table 25 WLAN Key Management Requirements**

| Req#       | Requirement Description   | Threshold/<br>Objective |
|------------|---|-------------------------|
| WLAN-KM-25 | Certificate revocation information shall be made available by posting the data to a repository or service that is available for the WLAN Authentication Server.   | T=O                     |
| WLAN-KM-26 | The WLAN CA shall issue certificates to the WLAN Authentication Server that contains the TLS Web Server Authentication OID (1.3.6.1.5.5.7.3.1) in the ExtendedKeyUsage extension.   | T=O                     |
| WLAN-KM-27 | The WLAN CA shall not issue certificates that contain the TLS Web Server Authentication OID (1.3.6.1.5.5.7.3.1) in the ExtendedKeyUsage extension to any devices other than the WLAN Authentication Server and Wireless System. | T=O                     |
| WLAN-KM-28 | The WLAN CA shall issue certificates to WLAN Clients that contain the Client Authentication OID (1.3.6.1.5.5.7.3.2) in the ExtendedKeyUsage field. Reference is RFC 5216 EAP-TLS, Sect 5.3, March 2008.                         | T=O                     |
| WLAN-KM-29 | Locally-run WLAN CAs shall only issue certificates to WLAN Clients, the WLAN Authentication Server, or to support its own operations.   | T=O                     |
| WLAN-KM-30 | Locally-run red network CAs shall only issue certificates to Inner VPN Components of CSfC Solutions or to support its own operation.  | T=O                     |
| WLAN-KM-31 | Certificate revocation information shall be made available by posting the data to a repository or service that is available for the WLAN Authentication Server.   | T=O                     |
| WLAN-KM-32 | The WLAN CA shall be connected to the Gray Management Network   | T=O                     |
| WLAN-KM-33 | Inner VPN Components shall only trust an Inner tunnel CA used within the solution.  | T=O                     |
| WLAN-KM-34 | WLAN Components shall only trust an Gray Management Network CA used within the solution.  | T=O                     |

| WLAN-KM-35 | All public/private key pairs and certificates for VPN Components shall | T=O |
|------------|--|-----|
|            | be used for authentication only.                                       |     |

# **10.16** Provisioning Requirements

# **10.16.1** End User Device Provisioning Requirements

## **Table 26 End User Device Provisioning Requirements**

| Req #      | Requirement Description  | Threshold/<br>Objective |
|------------|--|-------------------------|
| WLAN-PR-1  | A Provisioning WLAN using WPA2-PSK authentication and encryption shall be established on the Gray Management network to support wireless provisioning of EUDs.   | Т                       |
| WLAN-PR-2  | A Provisioning WLAN using WPA2-PSK authentication and encryption shall be established on the Red network to support wireless provisioning of EUDs.   | Т                       |
| WLAN-PR-3  | The Provisioning WLAN on the Gray Management Network shall be contained within a shielded enclosure that provides 100 dB of attenuation across the frequency range from 2 to 6 GHz.  | Т                       |
| WLAN-PR-4  | The Provisioning WLAN on the Red network shall be contained within a shielded enclosure that provides 100 dB of attenuation across the frequency range from 2 to 6 GHz.  | Т                       |
| WLAN-PR-5  | EUDs shall be provisioned over the Provisioning WLANs (or meet WLAN-PR-6).   | Т                       |
| WLAN-PR-6  | EUDs shall be provisioned over wired connections.  | 0                       |
| WLAN-PR-7  | When a EUD has been successfully provisioned, its identity (ITU-T X.509v3 Distinguished Name or Subject Alternate Name) shall be recorded in authorization databases accessible to the WLAN Authentication Server and VPN Gateway. | T=O                     |
| WLAN-PR-8  | The authorization database shall be configured to remove or disable EUDs.  | T=O                     |
| WLAN-PR-9  | The EUD shall be loaded with an authorized software build during provisioning.   | T=O                     |
| WLAN-PR-10 | The EUD shall be loaded with WLAN and VPN configuration profiles during provisioning.  | T=O                     |
| WLAN-PR-11 | Password requirements for the EUD shall be established.  | T=O                     |
| WLAN-PR-12 | The EUD shall be provisioned to disable any unauthorized services.   | T=O                     |
| WLAN-PR-13 | The EUD shall be provisioned to generate and/or load keys and certificates (See separate key management requirements.)   | T=O                     |

# 11 GUIDANCE FOR USE AND HANDLING REQUIREMENTS

The roles required to administer and maintain the solution are defined below, along with doctrinal requirements for these roles.

**Security Administrator**—The Security Administrator should be responsible for maintaining, monitoring, and controlling all security functions for the entire suite of products composing the Campus IEEE 802.11 WLAN solution within a single site.

Security Administrator duties include but are not limited to:

- 1. Ensuring that the latest software patches and updates, to include IAVAs, are applied to each product.
- 2. Documenting and reporting security-related incidents to the appropriate authorities.
- 3. Coordinating and supporting product logistic support activities including integration and maintenance. Some logistic support activities may require that the Security Administrator escort uncleared personnel.
- 4. Employing adequate defenses of auxiliary network devices to enable proper and secure functionality of the Campus IEEE 802.11 WLAN Solution.
- 5. Ensuring that the implemented Campus IEEE 802.11 WLAN Solution remains compliant with the latest version of this Capability Package.
- 6. Monitoring the Wireless IDS logs on a regular basis (preferably full-time) to detect signs of attempted wireless intrusion attempts.
- Denying access by UEs by removing their identities from the WLAN and VPN authorization databases. This duty may include coordinating with the Certificate Authority Administrator (CAA) to revoke certificates.

**Certificate Authority Administrator (CAA)**—The CAA should be responsible for maintaining, monitoring, and controlling all security functions for the CA products. CAA duties include but are not limited to:

- 1. Administering the CA, including authentication of all devices requesting certificates.
- 2. Maintaining and updating the Certificate Revocation List or whitelist.
- 3. Notifying the Security Administrator of revoked certificates so they can be removed from WLAN and VPN authorization databases.

**Auditor**—The Auditor should be responsible for reviewing the actions performed by the Security Administrator and CAA and events recorded in the audit logs to ensure that no action or event represents a compromise to the security of the Campus IEEE 802.11 WLAN Solution. The role of Auditor and Security Administrator should not be performed by the same individual. The Auditor should only be allowed access to the Gray Management network and Red network administration devices. Auditor duties include but are not limited to:

- 1. Reviewing, managing, controlling, and maintaining security audit log data.
- 2. Documenting and reporting security-related incidents to the appropriate authorities.

**Solution Integrator**—In certain cases, an external integrator may be hired to implement a Campus IEEE 802.11 WLAN Solution based on this Capability Package. Solution Integrator duties may include but are not limited to:

- 1. Acquiring the products that compose the solution.
- 2. Configuring the Campus IEEE 802.11 WLAN Solution in accordance with this Capability Package.

# 11.1 Guidance for Use and Handling Requirements

The following requirements shall be followed regarding the use and handling of the solution.

**Table 27 Guidance for Use and Handling Requirements** 

| Req#       | Requirement Description   | Threshold/<br>Objective |
|------------|---|-------------------------|
| WLAN-GD-1  | All components of the solution when powered off shall be physically protected as classified devices, classified at the level of the network in the solution with the highest classification.  | Т                       |
| WLAN-GD-3  | Only authorized and appropriately cleared (or escorted) administrators and security personnel shall have physical access to the infrastructure components.  | T=O                     |
| WLAN-GD-4  | Only authorized and appropriately cleared users, administrators, and security personnel shall have physical access to EUDs.   | T=O                     |
| WLAN-GD-5  | All components of the solution shall be disposed of as classified devices, unless declassified using AO/DAA-approved procedures.  | T=O                     |
| WLAN-GD-6  | All EUDs shall have their certificates revoked prior to disposal.   | T=O                     |
| WLAN-GD-7  | Acquisition and procurement documentation shall not include information about how the equipment will be used, to include that it will be used to protect classified information.  | T=O                     |
| WLAN-GD-8  | The solution owner shall allow, and fully cooperate with, NSA or its authorized agent to perform an IA compliance audit (including, but not limited to, inspection, testing, observation, interviewing) of the solution implementation to ensure it meets the latest version of the Capability Package. | T=O                     |
| WLAN-GD-9  | The AO/DAA will ensure that a compliance audit shall be conducted every year against the latest version of the Campus WLAN Capability Package.  | T=O                     |
| WLAN-GD-10 | Results of the compliance audit shall be provided to and reviewed by the AO/DAA.  | T=O                     |
| WLAN-GD-11 | When a new approved version of the Campus WLAN Capability Package is published by NSA, the AO/DAA shall ensure compliance against this new Capability Package within 6 months.  | T=O                     |
| WLAN-GD-12 | Solution implementation information, which was provided to NSA during solution registration, shall be updated every 12 (or less) months.  | T=O                     |
| WLAN-GD-13 | Audit log data shall be maintained for a minimum of 1 year.   | T=O                     |
| WLAN-GD-14 | The amount of storage remaining for audit events shall be assessed quarterly in order to ensure that adequate memory space is available to continue recording new audit events.   | T=O                     |
| WLAN-GD-15 | Audit data shall be frequently offloaded to a backup storage medium.  | T=O                     |
| WLAN-GD-16 | A set of procedures shall be developed by the implementing organization to provide guidance for identifying and reporting security incidents associated with the audit events to the proper authorities and to the data owners.   | T=O                     |
| WLAN-GD-17 | The implementing organization shall develop a continuity of operations plan for auditing capability which includes a mechanism or method for determining when the audit log is reaching its maximum storage capacity.   | T=O                     |
| WLAN-GD-18 | The implementing organization shall develop a continuity of operations plan for auditing capability which includes a mechanism or method for off-loading audit log data for long- term storage.   | T=O                     |

| operations plan for auditing capability which includes a mechanism or method for responding to an overflow of audit log data within a product.  WLAN-GD-20  The implementing organization shall develop a continuity of operations plan for auditing capability which includes a mechanism or method for ensuring that the audit log can be maintained during power events. | Γ=0<br>Γ=0<br>Γ=0 |
|---|-------------------|
| operations plan for auditing capability which includes a mechanism or method for ensuring that the audit log can be maintained during power events.  WLAN-GD-21 Strong passwords shall be used that comply with the requirements of   | Г=О               |
|   |                   |
| the local security dutilioney.  | Г=О               |
| WLAN-GD-22 Security critical patches (such as IAVAs) shall be tested and subsequently applied to all components in the solution in accordance with local policy and this Capability Package.  |                   |
| WLAN-GD-23 Local policy shall dictate how the Security Administrator will install patches to solution components.   | Г=О               |
| WLAN-GD-24 Solution components shall comply with local TEMPEST policy.  | Г=О               |
| WLAN-GD-25 Users shall not establish a network or data connection from the EUD to a network other than through an authorized Campus WLAN connection.  | Γ=Ο               |
| WLAN-GD-26 Users shall not change, or attempt to change, the administrator-configured settings of the device.   | Г=О               |
| WLAN-GD-27 Users shall report loss, theft, deactivation, destruction, or suspected compromise (e.g., detected tamper) of devices in compliance with procedures established by the implementing organization.  | Г=О               |
| WLAN-GD-28  The Security Administrator, CAAs, Auditor, User, and all Solution Integrators shall be cleared to the highest level of data protected by the Campus WLAN solution. When an Enterprise CA is used in the solution, the CAA already in place may also support this solution, provided they meet this requirement.   | Γ=Ο               |
| WLAN-GD-29 The Security Administrator, CAA, and Auditor roles shall be performed by different people.   | Г=О               |
| the Outer tunnel.   | Г=О               |
| WLAN-GD-31 Upon discovering an EUD is lost or stolen, a User shall immediately report the incident to their System Administrator and Certificate Authority Administrator  | Г=О               |
| WLAN-GD-32 Upon notification of a lost or stolen EUD, the Certificate Authority Administrators shall revoke the EUD certificates and provide an updated CRL to the Security Administrator.  | Γ=Ο               |
| WLAN-GD-33 When an EUD's Certificate is revoked, the Security Administrator shall update the CRLs for the WLAN Authentication Server and the VPN Gateway.   | Γ=0               |

# 12 SOLUTION TESTING

This section provides a framework for a Test and Evaluation (T&E) plan and procedures to validate the implementation of a Campus WLAN solution. This T&E will be a critical part of the approval process for the AO/DAA, providing a robust body of evidence that shows compliance with this Capability Package.

The security features and operational capabilities associated with the use of the solution shall be tested. The following is a general high-level methodology for developing the test plan and procedures and for the execution of those procedures to validate the implementation and functionality of the Campus

WLAN solution. The entire solution, to include each component described in Section 6, is addressed by this test plan.

- 1) Set up the baseline network architecture and configure all components.
- 2) Document the baseline network architecture configuration. Include product model and serial numbers, and software version numbers as a minimum.
- 3) Develop a Test Plan for the specific implementation using the test objectives from Section 13. Any additional requirements imposed by the local AO/DAA should also be tested, and the Test Plan shall include tests to ensure that these requirements do not interfere with the security of this solution as described in this Capability Package.
- 4) Perform testing using the test plan derived in Step 3. Network testing will consist of both Black Box testing and Gray Box testing. A two-person testing approach should be used to administer the tests. During test execution, security and non-security related discrepancies with the solution shall be documented.
- 5) Compile findings, to include comments and vulnerability details as well as possible countermeasure information, into a Final Test Report to be delivered to the AO/DAA for approval of the solution.

The following testing requirement has been developed to ensure that the Campus WLAN solution functions properly and meets the configuration requirements from Section 10. Testing of these requirements should be used as a minimum framework for the development of the detailed test plan and procedures.

#### **Table 28 Testing Requirement**

| Req#      | Requirement Description  | Threshold /<br>Objective |
|-----------|--|--------------------------|
| WLAN-TR-1 | The organization implementing the Capability Package shall perform all tests listed in Section 13. | T=O                      |

## **13 TEST CRITERIA**

This section contains the specific tests that allow the Security Administrator or System Integrator to ensure that they have properly configured the solution. These tests may also be used to provide evidence to the AO/DAA regarding compliance of the solution with this Capability Package. Note that the details of the procedures are left up to the final developer of the test plain in accordance with AO/DAA-approved network procedures. The AO/DAA is ultimately responsible for ensuring that all requirements from the Capability Package have been properly implemented.

#### 13.1 Wireless Connection Establishment Protocols

This test procedure verifies that the correct protocols are used when a WLAN Client joins the wireless network.

Requirements being tested: WLAN-WL-5, WLAN-WC-5, WLAN-AA-1, WLAN-AA-2, WLAN-WS-2, WLAN-IA-1, WLAN-WA-8

#### **Procedure Description:**

- 1) Set up an IEEE 802.11 sniffer and configure it to operate in promiscuous mode.
- 2) Set up a packet sniffer on the network connection between the Wireless System and the WLAN Authentication Server and configure it to operate in promiscuous mode.
- 3) Either temporarily disable the use of IPsec on the connection between the Wireless System and the WLAN Authentication Server, or provide a copy of the pre-shared key between the two to the packet sniffer. (This is necessary to allow the packet sniffer to inspect the authentication traffic between the two components.)
- 4) For each EUD, perform the following:
  - a) Enable the sniffers.
  - b) Power on the EUD.
  - c) Establish a connection between the EUD and the wireless network.
  - d) Disable the sniffers.
  - e) Shut down the EUD.
  - f) Examine the IEEE 802.11 capture to verify that all wireless traffic between the WLAN Client and the Wireless System is following the WPA2-Enterprise protocol. (WLAN-WL-5)
  - g) Examine the packet capture to verify that all EAP messages in transit between the Wireless
     System and the WLAN Authentication Server are encapsulated in RADIUS messages. (WLAN-IA-1)
  - h) Compare the EAP messages in the IEEE 802.11 capture and the packet capture to verify that they are identical. (WLAN-WS-2)
  - i) Examine the EAP messages in the IEEE 802.11 capture to verify that EAP-TLS is being used as the authentication protocol. (WLAN-AA-1)
  - j) Examine the EAP-TLS messages in the IEEE 802.11 capture to verify that the negotiated TLS cipher suite specifies CBC as the cipher mode. (WLAN-AA-2)
  - k) Examine the EAP-TLS messages in the IEEE 802.11 capture to verify that the WLAN Client presents its device certificate during TLS negotiation. (WLAN-WC-5)
  - I) Examine the EAP-TLS messages in the IEEE 802.11 capture to verify that the WLAN Authentication Server presents its device certificate during TLS negotiation. (WLAN-WA-8)
- 5) Re-enable IPsec on the connection between the Wireless System and the WLAN Authentication Server, if it had been disabled in Step 3.
- 6) Remove the sniffers.

## **Expected Result:**

In steps 4(f)-(I), the captures should reveal that the correct protocols are being used during WLAN authentication.

## 13.2 Wireless Infrastructure Authentication Protocols

This test procedure verifies that the correct protocols and algorithms are used to protect authentication traffic between the Wireless System and the WLAN Authentication Server.

Requirements being tested: WLAN-IA-1, WLAN-IA-2, WLAN-IA-3, WLAN-IA-4, WLAN-IA-5, WLAN-IA-6, WLAN-IA-7, WLAN-IA-8, WLAN-IA-10, WLAN-IA-11, WLAN-IA-12, WLAN-IA-13, WLAN-IA-14, WLAN-IA-15, WLAN-IA-19

- 1) Set up a packet sniffer on the network connection between the Wireless System and the WLAN Authentication Server and configure it to operate in promiscuous mode.
- 2) Enable the sniffer.
- 3) Power on the Wireless System and the WLAN Authentication Server.
- 4) Wait until the Wireless System and the WLAN Authentication Server have established an IPsec tunnel and are communicating through it.
- 5) Disable the sniffer.
- 6) Examine the packet capture to verify that all of the messages between the Wireless System and the WLAN Authentication Server are either IKE or IPsec. (WLAN-IA-1)
- 7) Examine the IKE messages in the packet capture to verify each of the following:
  - a) That IKEv1 is being used in Main Mode on Phase 1. (WLAN-IA-2)
  - b) That IKEv2 is being used. (WLAN-IA-3)
  - c) That the Wireless System and WLAN Authentication Server agree to use DH Group 14 during the IKE exchange. (WLAN-IA-4)
  - d) That the Wireless System and WLAN Authentication Server agree to use DH Group 19 and/or 20 during IKE exchange (WLAN-IA-19).
  - e) That the Wireless System and WLAN Authentication Server agree to use SHA-1 during the IKE exchange. (WLAN-IA-5)
  - f) That the Wireless System and WLAN Authentication Server agree to use protocols and algorithms selected from Table A-8 that are approved to protect the highest classification level of the Red Network data during the IKE exchange. (WLAN-IA-7)
  - g) That the Wireless System and WLAN Authentication Server agree to use protocols and algorithms selected from the Algorithm Suite for TS and Below in Table A-8 during the IKE exchange. (WLAN-IA-8)
  - h) That the Wireless System and WLAN Authentication Server agree to use an IKE SA lifetime of 24 hours. (WLAN-IA-12)
  - i) That the Wireless System and WLAN Authentication Server agree to authenticate one another using a pre-shared key. (WLAN-IA-14)
  - j) That the Wireless System and WLAN Authentication Server agree to authenticate one another using X.509v3 certificates. (WLAN-IA-15)

- 8) On both the Wireless System and WLAN Authentication Server, examine the active ESP SAs to verify each of the following:
  - a) That the ESP SA between the Wireless System and the WLAN Authentication Server is using SHA 1. (WLAN-IA-6)
  - b) That the ESP SA between the Wireless System and the WLAN Authentication Server is using protocols and algorithms selected from Table A-8 that are approved to protect the highest classification level of the Red Network data. (WLAN-IA-7)
  - That the ESP SA between the Wireless System and the WLAN Authentication Server is using protocols and algorithms selected from the Algorithm Suite for TS and Below in Table A-8.
     (WLAN-IA-8)
  - d) That the ESP SA between the Wireless System and the WLAN Authentication Server is using AES in CBC mode. (WLAN-IA-10)
  - e) That the ESP SA between the Wireless System and the WLAN Authentication Server is using AES in GCM mode. (WLAN-IA-11)
  - f) That the ESP SA between the Wireless System and the WLAN Authentication Server has a lifetime of 8 hours. (WLAN-IA-13)

In step 6, the packet capture should show that all traffic between the Wireless System and the WLAN Authentication System is either IKE or IPsec. In step 7, the packet capture should show that the IKE exchange has been configured properly. In step 8, the status of the two components should show that the ESP SA has been configured properly.

# 13.3 Extended Key Usage Extension Checking by WLAN Client

This test procedure verifies that the WLAN Client is checking the Extended Key Usage extension of the WLAN Authentication Server's TLS certificate.

Requirements being tested: WLAN-WC-11

- Generate a TLS certificate that does not contain the TLS Web Server Authentication Object Identifier (id-kp-serverAuth 1.3.6.1.5.5.7.3.1) in the Extended Key Usage extension and load it onto the WLAN Authentication Server.
- 2) For each EUD, perform the following:
  - a) Power on the EUD.
  - b) Verify that the EUD is unable to connect to the WLAN. (WLAN-WC-11)
  - c) Shut down the EUD.
- 3) Generate a TLS certificate that *does* contain the TLS Web Server Authentication Object Identifier (id-kp-serverAuth 1.3.6.1.5.5.7.3.1) in the Extended Key Usage extension and load it onto the WLAN Authentication Server.
- 4) For each EUD, perform the following:

- a) Power on the EUD.
- b) Verify that the EUD is able to connect to the WLAN. (WLAN-WC-11)
- c) Shut down the EUD.

In step 2(b), each EUD should fail to connect to the WLAN. In step 4(b), each EUD should be able to connect to the WLAN.

# 13.4 Extended Key Usage Extension Checking by WLAN Authentication Server

This test procedure verifies that the WLAN Authentication Server is checking the Extended Key Usage extension of the WLAN Client's TLS certificate.

Requirements being tested: WLAN-WA-6

#### **Procedure Description:**

- 1) Generate a TLS certificate that does *not* contain the TLS Client Authentication Object Identifier (1.3.6.1.5.5.7.3.2) in the Extended Key Usage extension and load it onto an EUD's WLAN Client.
- 2) Power on the EUD.
- 3) Verify that the EUD is unable to connect to the WLAN. (WLAN-WA-6)
- 4) Shut down the EUD.
- 5) Generate a TLS certificate that *does* contain the TLS Client Authentication Object Identifier (1.3.6.1.5.5.7.3.2) in the Extended Key Usage extension and load it onto the EUD's WLAN Client.
- 6) Power on the EUD.
- 7) Verify that the EUD is able to connect to the WLAN. (WLAN-WA-6)
- 8) Shut down the EUD.

#### **Expected Result:**

In step 3, the EUD should fail to connect to the WLAN. In step 7, the EUD should be able to connect to the WLAN.

# 13.5 Authentication Server Name Checking by WLAN Client

This test procedure verifies that the WLAN Clients are checking the Distinguished Name and Subject Alternate Name attributes of the WLAN Authentication Server certificate during authentication.

Requirements being tested: WLAN-WC-3

- Generate a TLS certificate that does not contain values in the Distinguished Name and Subject Alternative Name fields that appear in the whitelist used by the WLAN Clients, and load the certificate onto the WLAN Authentication Server.
- 2) For each EUD, perform the following:
  - a) Power on the EUD.

- b) Verify that the EUD is unable to connect to the WLAN. (WLAN-WC-3)
- c) Shut down the EUD.
- 3) Generate a TLS certificate that does contain values in the Distinguished Name and Subject Alternative Name fields that appear in the whitelist used by the WLAN Clients, and load the certificate onto the WLAN Authentication Server.
- 4) For each EUD, perform the following:
  - a) Power on the EUD.
  - b) Verify that the EUD is able to connect to the WLAN. (WLAN-WA-7)
  - c) Shut down the EUD.

In step 2(b), the EUDs should fail to connect to the WLAN. In step 4(b), the EUDs should be able to connect to the WLAN.

# 13.6 Client Name Checking by WLAN Authentication Server

This test procedure verifies that the WLAN Authentication Server is checking the Distinguished Name and Subject Alternate Name attributes of WLAN Client certificates during authentication.

Requirements being tested: WLAN-WA-7

## **Procedure Description:**

- 1) Generate a TLS certificate that does *not* contain values in the Distinguished Name and Subject Alternative Name fields that appear in the whitelist used by the WLAN Authentication Server, and load the certificate onto an EUD's WLAN Client.
- 2) Power on the EUD.
- 3) Verify that the EUD is unable to connect to the WLAN. (WLAN-WA-7)
- 4) Shut down the EUD.
- 5) Generate a TLS certificate that *does* contain values in the Distinguished Name and Subject Alternative Name fields that appear in the whitelist used by the WLAN Authentication Server, and load the certificate onto the EUD's WLAN Client.
- 6) Power on the EUD.
- 7) Verify that the EUD is able to connect to the WLAN. (WLAN-WA-7)
- 8) Shut down the EUD.

#### **Expected Result:**

In step 3, the EUD should fail to connect to the WLAN. In step 7, the EUD should be able to connect to the WLAN.

# 13.7 Root Certificate Authority Checking by WLAN Client

This test procedure verifies that the WLAN Client checks that the WLAN Authentication Server's certificate is rooted by a trusted CA.

Requirements being tested: WLAN-WC-2

#### **Procedure Description:**

- 1) Generate a TLS certificate whose signature chain is *not* rooted by the Root CA for the Gray network and load it onto the WLAN Authentication Server.
- 2) For each EUD, perform the following:
  - a) Power on the EUD.
  - b) Verify that the EUD is unable to connect to the WLAN. (WLAN-WC-2)
  - c) Shut down the EUD.
- 3) Generate a TLS certificate whose signature chain *is* rooted by the Root CA for the Gray network and load it onto the WLAN Authentication Server.
- 4) For each EUD, perform the following:
  - a) Power on the EUD.
  - b) Verify that the EUD is able to connect to the WLAN. (WLAN-WC-2)
  - c) Shut down the EUD.

#### **Expected Result:**

In step 2(b), each EUD should fail to connect to the WLAN. In step 4(b), each EUD should be able to connect to the WLAN.

#### 13.8 Ad Hoc Mode

This test procedure checks that WLAN Clients do not attempt to use ad hoc mode.

Requirements being tested: WLAN-WC-8

- 1) Set up an IEEE 802.11 sniffer and configure it to operate in promiscuous mode.
- 2) Set up a host (workstation, laptop, etc.) other than an EUD to operate in ad hoc mode.
- 3) Turn off the Wireless System.
- 4) For each EUD, perform the following:
  - a) Enable the sniffer.
  - b) Power on the EUD.
  - c) Verify that the EUD does not attempt to engage in ad hoc mode with the host set up in Step 1. (WLAN-WC-8)
  - d) Shut down the EUD.
  - e) Disable the sniffer.
  - f) Examine the IEEE 802.11 capture to verify that the EUD did not transmit any frames attempting to communicate with the host in ad hoc mode. (WLAN-WC-8)

In steps 4(c) and 4(f), each EUD should fail to use ad hoc mode to communicate with the other host.

#### 13.9 Unauthorized SSIDs

This test procedure checks that WLAN Clients do not attempt to join networks other than those with authorized SSIDs.

Requirements being tested: WLAN-WC-10

#### **Procedure Description:**

- 1) Set up an IEEE 802.11 sniffer and configure it to operate in promiscuous mode.
- 2) Configure the Wireless System to broadcast an unauthorized SSID value.
- 3) For each EUD, perform the following:
  - a) Enable the sniffer.
  - b) Power on the EUD.
  - c) Verify that the EUD does not attempt to connect to the wireless network. (WLAN-WC-10)
  - d) Shut down the EUD.
  - e) Disable the sniffer.
  - f) Examine the IEEE 802.11 capture to verify that the EUD did not transmit any frames attempting to connect to a wireless network. (WLAN-WC-10)
- 4) Configure the Wireless System to broadcast an authorized SSID value.
- 5) For each EUD, perform the following:
  - a) Power on the EUD.
  - b) Verify that the EUD successfully connects to the wireless network. (WLAN-WC-10)
  - c) Shut down the EUD.

#### **Expected Result:**

In steps 3(c) and 3(f), each EUD should not attempt to join the wireless network when it broadcasts the incorrect SSID. In step 5(b), each EUD should successfully connect to the wireless network when it broadcasts the correct SSID.

#### 13.10 Authentication Methods Other Than EAP-TLS

This test procedure verifies that the WLAN Authentication Server will not allow any authentication methods other than EAP-TLS.

Requirements being tested: WLAN-WA-1

- 1) For one or more authentication methods other than EAP-TLS (e.g. EAP-MD5, EAP-PSK, EAP-FAST, etc.):
  - a) Configure a host to authenticate using the selected authentication method.

- b) Verify that the host is unable to connect to the network. (WLAN-WA-1)
- 2) Power on a (properly configured) EUD.
- 3) Verify that the EUD is able to connect to the network. (WLAN-WA-1)

In step 1(b), the host should be unable to connect to the network using an authentication method other than EAP-TLS. In step 3, the EUD should be able to connect to the network using EAP-TLS.

#### 13.11 Authorization Check of WLAN Client Certificate

This test procedure verifies that the WLAN Authentication Server only allows a WLAN Client to connect if its certificate is still valid.

Requirements being tested: WLAN-WA-3, WLAN-KM-31

#### **Procedure Description:**

- 1) Revoke the WLAN Client certificate of an EUD, such as by adding it to a CRL or removing it from a whitelist.
- 2) Instruct the WLAN Authentication Server to retrieve updated certificate revocation information. (WLAN-KM-31)
- 3) Power on the EUD with the revoked certificate.
- 4) Verify that the EUD is unable to connect to the network. (WLAN-WA-3)
- 5) Power on an EUD whose WLAN Client certificate has not been revoked.
- 6) Verify that this EUD is able to connect to the network. (WLAN-WA-3)

#### **Expected Result:**

In step 2, the WLAN Authentication Server should be able to obtain current certificate status information. In step 4, an EUD whose WLAN Client certificate has been revoked should not be able to connect to the network. In step 6, an EUD whose WLAN Client certificate is still valid should be able to connect to the network.

#### 13.12 WLAN Client Automatic Establishment

This test procedure verifies that the WLAN Client on an EUD automatically connects to the WLAN at start-up.

Requirements being tested: WLAN-WC-1

#### **Procedure Description:**

- 1) Power on an EUD.
- 2) Do not interact with the EUD, except to respond to any authentication prompts that may appear.
- 3) Verify that the EUD has connected to the WLAN. (WLAN-WC-1)

#### **Expected Result:**

In step 3, the EUD should connect to the WLAN without having been specifically instructed to do so by the tester.

#### 13.13 WLAN Client Certificates

This test procedure verifies that each EUD has been configured with appropriate WLAN Client certificates.

Requirements being tested: WLAN-WC-4, WLAN-WC-12

#### **Procedure Description:**

- 1) For each EUD, perform the following:
  - a) Verify that its WLAN Client has been loaded with a device certificate that has not been loaded on any other EUD or other component in the system. (WLAN-WC-4)
  - b) Verify that its WLAN Client has been loaded with a CA (signing) certificate that can be used to verify the signature on the device certificate. (WLAN-WC-4)
  - c) Verify that its WLAN Client's device certificate has an extendedKeyUsage field that indicates support for Client Authentication (OID 1.3.6.1.5.5.7.3.2). (WLAN-WC-12)

#### **Expected Result:**

In step 1, the device certificate used by each EUD's WLAN Client should adhere to the desired properties.

# 13.14 WLAN Authentication Server Certificate

This test procedure verifies that the WLAN Authentication Server has been configured with an appropriate certificate.

Requirements being tested: WLAN-WA-2, WLAN-WA-5

#### **Procedure Description:**

- 1) Verify that the WLAN Authentication Server has been loaded with a device certificate that has not been loaded on any other component in the system. (WLAN-WA-2)
- 2) Verify that the WLAN Authentication Server has been loaded with a CA (signing) certificate that can be used to verify the signature on its device certificate. (WLAN-WA-2)
- 3) Verify that the WLAN Authentication Server's device certificate has an extendedKeyUsage field that indicates support for Server Authentication (OID 1.3.6.1.5.5.7.3.1). (WLAN-WA-5)

#### **Expected Result:**

In steps 1-3, the device certificate used by the WLAN Authentication Server should adhere to the desired properties.

# 13.15 Wireless System Certificate

This test procedure verifies that the Wireless System has been configured with an appropriate certificate.

Requirements being tested: WLAN-WS-5

#### **Procedure Description:**

- 1) Verify that the Wireless System has been loaded with a device certificate that has not been loaded on any other component in the system. (WLAN-WS-5)
- 2) Verify that the Wireless System has been loaded with a CA (signing) certificate that can be used to verify the signature on its device certificate. (WLAN-WS-5)

#### **Expected Result:**

In steps 1-2, the device certificate used by the Wireless System should adhere to the desired properties.

## 13.16 WLAN Infrastructure Design Review

This test procedure verifies that the design of the WLAN infrastructure meets the requirements of the CP.

#### Requirements being tested: WLAN-WC-13, WLAN-WS-1, WLAN-WS-4 Procedure Description:

- 1) Verify that all components used to manage WLAN Clients are physically connected only to the Gray Management Network. (WLAN-WC-13)
- 2) Inspect the physical operating environment of the wireless network to verify that there are no access points for an unclassified WLAN. (WLAN-WS-1)
- 3) Review the architecture of the system to verify that it only provides wireless access to Red networks of a single classification level. (WLAN-WS-4)
- 4) Review the configuration of the Wireless System to verify that it does not contain any pre-shared keys. (WLAN-IA-18)

#### **Expected Result:**

In step 1, WLAN Clients should only be managed from the Gray Management Network. In step 2, there should be no unclassified WLAN operating in the same spaces as the system. In step 3, there should only be Red networks of a single classification level connected to the overall system. In steps 4 and 5, there should be no pre-shared keys between the Wireless System and the WLAN Authentication Server.

#### 13.17 WLAN Infrastructure Process Review

This test procedure verifies that the necessary processes for managing the WLAN infrastructure have been defined.

Requirements being tested: WLAN-IA-16, WLAN-WA-4

#### **Procedure Description:**

- Ask the Security Administrator for a copy of the composition rules for the pre-shared keys between the Wireless System and the WLAN Authentication Server, and verify that the rules exist. (WLAN-IA-16)
- 2) Ask the Security Administrator for a copy of the procedures for providing CRLs to the WLAN Authentication Server, and verify that they ensure that new CRLs are loaded before the old CRL expires. (WLAN-WA-4)

#### **Expected Result:**

In step 1, there should be composition rules for the pre-shared key. In step 2, there should be a mechanism for keeping the CRL on the WLAN Authentication Server current.

# 13.18 WLAN Client Certificate Expiration Notification

This test procedure verifies that WLAN Clients notify the EUD's user that its certificate is about to expire.

Requirements being tested: WLAN-WC-6

#### **Procedure Description:**

- 1) Identify the amount of advance notice users should receive before their EUD's WLAN Client certificate expires.
- 2) For each EUD, perform the following:
  - a) Generate a TLS certificate with a lifetime of five minutes plus the amount of time identified in Step 1 and load it onto the EUD's WLAN Client.
  - b) Wait five minutes.
  - c) Verify that the WLAN Client has alerted the user that its device certificate is due to expire. (WLAN-WC-6)

# 13.19 Pre-Shared Key Entropy Test

This test procedure verifies that the pre-shared key between the Wireless System and the WLAN Authentication Server is generated with sufficient entropy.

Requirements being tested: WLAN-IA-17

#### **Procedure Description:**

- 1) Generate a large number of keys using the same process used to produce the pre-shared key between the Wireless System and the WLAN Authentication Server.
- 2) Use the NIST Statistical Test Suite and NIST SP 800-22 to evaluate the randomness of the keys generated in Step 1.
- 3) Verify that the output of Step 2 indicates that the keys each have a minimum of 256 bits (for Top Secret and below) or 128 bits (for Second and below) of entropy. (WLAN-IA-17)

#### **Expected Result:**

In step 3, the keys should have the appropriate level of entropy for the classification of the system.

# 13.20 WLAN Cryptographic Algorithms

This test procedure verifies that the WLAN Clients and Wireless System are configured to use the correct set of cryptographic algorithms to protect data in transit.

Requirements being tested: WLAN-WL-1, WLAN-WL-2, WLAN-WL-3, WLAN-WL-4, WLAN-WL-6, WLAN-WL-7, WLAN-WC-7, WLAN-WS-3

### **Procedure Description:**

1) Examine the Wireless System's configuration to verify that it is configured to use AES Key Wrap instead of RC4 Encryption for protecting WPA2 keys in transit. (WLAN-WL-6, WLAN-WL-7)

- 2) Examine the Wireless System's configuration to verify that it is configured to use only the protocols and algorithms selected from the appropriate column of Table A-8 or A-9, based on the date and the highest classification level of data on the Red network. (WLAN-WL-1, WLAN-WL-2, WLAN-WL-3, WLAN-WL-4)
- 3) Examine the Wireless System's configuration to verify that it is configured to negotiate new session keys with WLAN Clients at least once per hour. (WLAN-WS-3)
- 4) For each EUD, perform the following:
  - a) Power on the EUD.
  - b) Verify that the EUD is able to connect to the WLAN. (WLAN-WL-1, WLAN-WL-2, WLAN-WL-3, WLAN-WL-4, WLAN-WL-6, WLAN-WL-7)
  - c) Leave the EUD connected for at least one hour.
  - d) Verify that the EUD has not been disconnected from the WLAN. (WLAN-WC-7)

In steps 1-3, the Wireless System should be configured correctly per the requirements of this CP. In steps 4(b) and 4(d), each EUD's WLAN Client should be configured similarly; otherwise, they would be unable to connect and stay connected to the WLAN.

## 13.21 WLAN Bridging

This test procedure verifies that the EUDs cannot be used to bridge the WLAN to an external network.

Requirements being tested: WLAN-WC-9

#### **Procedure Description:**

- 1) For each EUD, perform the following:
  - a) Inspect the EUD's networking configuration to verify that only one physical network interface is enabled. (WLAN-WC-9)

## **Expected Result:**

In step 1(a), the EUD should be unable to connect to two different networks simultaneously.

#### 13.22 Product Selection

This section contains a procedure to verify that the Inner and Outer components were selected to ensure independence in several important features.

Requirements being tested: WLAN-PS-1 through WLAN-PS-17

- 1) For each Inner and Outer Component, perform the following:
  - a) Inspect that the Wireless System and VPN Gateway came from different vendors and that the vendors are not a subsidiary of each other. (WLAN-PS-1).
  - b) Inspect that the WLAN Authentication Server and VPN Gateway came from different vendors and that the vendors are not a subsidiary of each other. (WLAN-PS-2)

- c) Inspect that the WLAN Client and VPN Client came from different vendors and that the vendors are not a subsidiary of each other. (WLAN-PS-3)
- d) Inspect that the WLAN Authentication Server and the VPN Client came from different vendors and that the vendors are not a subsidiary of each other. (WLAN-PS-4)
- e) Inspect that the Wireless System and VPN Client came from different vendors and that the vendors are not a subsidiary of each other. (WLAN-PS-5)
- f) Inspect that the VPN Gateway and WLAN Client came from different vendors and that the vendors are not a subsidiary of each other. (WLAN-PS-6)
- g) Inspect that the WLAN CA and VPN CA came from different vendors and that the vendors are not a subsidiary of each other. (WLAN-PS-7)
- h) Inspect the configuration files to verify that the WLAN Authentication Server is logically separated from the Wireless System. (WLAN-PS-8)
- i) Inspect that the VPN Gateway is physically separated from the WLAN Authentication Server and Wireless System. (WLAN-PS-9)
- j) Verify that the WLAN Authentication Server is physically separated from the Wireless System. (WLAN-PS-9)
- k) Inspect that the VPN Client and WLAN Client run on different operating systems on the EUD. (WLAN-PS-10)
- I) Inspect that the WLAN Controller and VPN Gateway run on different Operating Systems for critical IA security functionality. (WLAN-PS-11)
- m) Inspect that each component comes from the CSFC Component List. (WLAN-PS-12)
- n) Verify that all components go through a Supply Chain Threat Assessment and necessary mitigations are implemented for component vulnerabilities. (WLAN-PS-13)
- o) Inspect that Wireless System and VPN Gateway cryptographic libraries are different implementations. (WLAN-PS-14)
- p) Inspect that the WLAN Client and VPN Client cryptographic libraries are different implementations. (WLAN-PS-15)
- q) Inspect that the WLAN CA and the VPN CA cryptographic libraries are different implementations. (WLAN-PS-16)

The results of the inspection should reveal that the Campus WLAN components conform to the Campus WLAN CP; results are pass/fail.

## 13.23 End User Device Configurations

This section contains procedures to ensure that the configuration for all the EUDs in the Campus WLAN solution follow the requirements given in this Capability Package.

Requirements being tested: WLAN-EU-1 through WLAN-EU-20

- 1) As a normal user attempt to change the EUD's network configuration authentication. (WLAN-EU-1)
- 2) Identify all the different password protections for the EUD. Ensure that the protections that require administrative access do not share a password with normal user password. (WLAN-EU-2)
- 3) Obtain a list of approved software for the EUD and verify that the EUD only has approved software on device. (WLAN-EU-3)
- 4) As a normal user attempt to remove/install software located on the EUD. (WLAN-EU-4)
- 5) Verify that the EUD requires authentication prior to gaining access to the device. (WLAN-EU-5)
- 6) Inspect the EUD's configuration file for number of log-in attempts. As a normal user verify by logging into the EUD with an incorrect password erases the data or locks the device for a period of time. (WLAN-EU-6)
- 7) Inspect the EUD's configuration file for screen lock time. As a normal user verify that the device requires authentication after a period of inactivity. (WLAN-EU-7)
- 8) Inspect the EUD's WLAN and VPN connection status. (WLAN-EU-8)
- 9) Inspect the EUD's management services and verify the network authorized to manage the device is "Campus WLAN". (WLAN-EU-9)
- 10) Connect the EUD to the WLAN but not the VPN. Verify that no application services are available until the VPN connection is established. (WLAN-EU-10)
- 11) Obtain the configuration file of the EUD and verify that WLAN and VPN encryption services are enabled. (WLAN-EU-11)
- 12) As a normal user attempt to disabled the WLAN and VPN encryption services on the EUD. (WLAN-EU-12)
- 13) Obtain the configuration file of the EUD and verify that the all wireless capabilities except 802.11 are disabled. (WLAN-EU-13)
- 14) Inspect that the EUD has full disk encryption. (WLAN-EUD-14)
- 15) Obtain the firewall configuration file on the EUD and verify that IKE, IPsec, and WPA2 are the only authorized authentication traffic. (WLAN-EUD-15)
- 16) Verify that the EUD contains a Trusted Platform Module (TPM) and that the TPM is enabled. (WLAN-EU-16)
- 17) Obtain the EUD's configuration file to verify that host-based services are enabled. (WLAN-EU-17)
- 18) Inspect the EUD for tamper seals are installed. (WLAN-EU-18)
- 19) Inspect the organization's EUD policy to verify if that the EUD should be treated classified at all times if the EUD does not have an NSA-approved DAR solution (WLAN-EU-19).
- 20) Inspect the organization's EUD policy to verify that it states that the EUD shall be re-provisioned if the device has been compromised (WLAN-EU-20).

The results of the inspection should reveal that the EUDs conform to the Campus WLAN CP; results are pass/fail.

# 13.24 Implementation of Guidance

This section ensures that there are procedures in place and/or that procedures were followed regarding that procurement of products and use of the Campus WLAN solution. It also ensures that the personnel in place to manage and administer this solution follow the guidelines given in this Capability Package.

Requirements being tested: WLAN-GD-1 through WLAN-GD-33

#### **Procedure Description:**

- 1) Verify procedures WLAN-GD-1 through 7, WLAN-GD-10, WLAN-GD-13 through WLAN-GD-28, and WLAN-GD-31 through WLAN-GD-33 were/are followed and/or currently in place.
- 2) Verify that the solution owner understands that he/she shall allow and fully cooperate with an NSA-ordered IA compliance audit of this solution implementation. (WLAN-GD-8)
- 3) Verify that the solution owner and AO/DAA are aware that a compliance audit shall be conducted every year against the latest Campus WLAN Capability Package. (WLAN-GD-9)
- 4) Verify that the solution owner and AO/DAA are aware that when a new version of the Campus WLAN Capability Package is published by the NSA, they will have 6 months to move into compliance with this new version. (WLAN-GD-11)
- 5) Verify that the solution owner and the AO/DAA are aware that solution implementation information provided during NSA solution registration is updated every year. (WLAN-GD-12)
- 6) Verify the personnel requirements given in WLAN-GD-29 through WLAN-GD-30 are met by the personnel supporting this implementation of the Campus WLAN.

#### **Expected Result:**

For steps 1-6, all of these procedures have been followed or are in place.

# 13.25 Implementation of Solution

This section ensures that create an accurate record of components composing the Campus WLAN solution.

Requirements being tested: WLAN-SR-1 through WLAN-SR-9

- 1) Log into each component and verify that all default accounts, passwords, community string, and other default access controls mechanisms are removed or changed. (WLAN-SR-1)
- 2) Ensure the Gray management network traffic is cryptographically or physically separate from the data on the Gray network. (WLAN-SR-2)
- 3) Log into each component and verify the default, self-signed or proprietary devices certificates are removed. (WLAN-SR-3)
- 4) Log into each component and verify that any built-in, pre-loaded trusted loaded CAs records are removed. (WLAN-SR-4)

- 5) Log into the Inner VPN Gateway and each component within the Red Network and verify that the time of day is synchronized with the same time source located in the Red network. (WLAN-SR-5)
- 6) Log into the WLAN Authentication Server, WLAN Controller, and all components within the Gray network and verify that the time of day is synchronized with the same time source located in the Gray Management network. (WLAN-SR-6)
- 7) Obtain the configuration files from each component and verify that the components adhere to local policy and U.S. Government guidance. (WLAN-SR-7)
- 8) Verify that the private key store on each component is protected by a password of sufficient length and complexity. (WLAN-SR-9)

For steps 1-9, the Campus WLAN solution components conform to the Campus WLAN CP.

# 13.26 Provisioning of the EUD

This section ensures the provisioning of the EUD is secure composing the Campus WLAN solution.

Requirements being tested: WLAN-PR-1 through WLAN-PR-13

- 1) Identify the Provisioning WLAN network for the solution and verify that the network uses WPA2-PSK for authentication and encryption to established EUD's. (WLAN-PR-1)
- 2) Identify the Provisioning WLAN network for the solution and verify that the network uses WPA2-PSK for WLAN authentication. Log into the EUD to verify that WPA2-PSK is enabled and used to connect to the Provisioning WLAN network. (WLAN-PR-2)
- 3) Inspect the Provisioning WLAN located on the Gray Management network and ensure that the component is contained within a shielded enclosure. (WLAN-PR-3)
- 4) Inspect the Provisioning WLAN located on the Red network and ensure that the component is contained within a shielded enclosure. (WLAN-PR-4)
- 5) Verify the local policy to ensure that EUDs will be provisioned over the Provisioning WLANs. (WLAN-PR-5)
- 6) Verify the local policy to ensure that EUDs will be provisioned over the wired connections. (WLAN-PR-6)
- 7) After provisioning a EUD, log into authorization databases accessible to the WLAN Authentication Server and VPN Gateway to verify that the EUD's identity is present. (WLAN-PR-7)
- 8) Log into the authorization database and verify that an EUD is able to be removed or disabled. (WLAN-PR-8)
- 9) Review the authorize software policy and verify that EUD only contains the authorized software. (WLAN-PR-9)
- 10) Verify the provisioning policy states that the EUD will contain WLAN and a VPN configuration profiles during provisioning. (WLAN-PR-10)
- 11) Verify in local policy that password requirements must be established for EUDs. (WLAN-PR-11)

- 12) Obtain the configuration file for the EUDs and verify that unauthorized services are disabled. (WLAN-PR-12)
- 13) Verify in local policy that during the provisioning of the EUDs, the device is able to generate and/or load keys and certificates. (WLAN-PR-13)

For steps 1-13, the provisioning of the EUDs adheres to the requirements found in this Capability Package.

## 13.27 Component Administration of the Solution

This section contains procedures to ensure that component administration for all Campus WLAN components follow the requirements given in this Capability Package.

Requirements being tested: WLAN-RA-1 through WLAN-RA-9

#### **Procedure Description:**

- 1) Log into each system component and verify that administration can only take place either by physical access or remotely using SSHv2, IPsec, or TLS. (WLAN-RA-1)
- 2) Obtain the configuration file for each components and if SSHv2, IPsec, TLS is used for remote management then these protocols must adhere to the appropriate RFCs. (WLAN-RA-2, WLAN-RA-3, WLAN-RA-4)
- 3) Obtain the administration workstation's configuration file and verify that antivirus software is enabled on the workstation. (WLAN-RA-6)
- 4) Obtain the configuration file for the WIDS and verify that the WIDS is encrypting and signing all alerts that are pushed to system administrator. (WLAN-RA-7)
- 5) Verify that the remote system administrator must authenticate to the WIDS. (WLAN-RA-8)
- 6) On each component within the Campus WLAN solution, verify that the IP address range for network administration is restricted to the range allowed by the client. (WLAN-RA-9)

#### **Expected Results:**

For steps 1-7, the administration of Campus WLAN solution components adheres to the requirements in this CP.

#### 13.28 Audit

This section contains procedure for ensuring audit events are detected, the proper information for each logged event, and there is a procedure detailed in the CPS documentation for auditing each CA device.

**Requirements being tested:** WLAN-AU-1 through WLAN-AU-16, WLAN-AU-18 through WLAN-AU-28, WLAN-AU-30 through WLAN-AU-32

## **Procedure Description:**

1) Examples for testing the ability of each Campus WLAN component to audit and log audit events specified in the CP are given below. Verify that for each event logged, the applicable data regarding the event is recorded for the log entry.

- a) The following actions are performed on the audit log. (WLAN-AU-1)
  - i) Log into the Administration Workstation as an administrator to the VPN Gateway.
  - ii) Delete an entry in the audit log.
  - iii) Verify that a log entry was created for the deletion of the audit log in step ii.
  - iv) Repeat the above instruction with the Auditor role.
- b) All actions performed by a user with super privileges (auditor, administrator, etc.) and any escalation of user privileges. (WLAN-AU-2, WLAN-AU-4, WLAN-AU-5)
  - i) Log into the Administration Workstation as an administrator to the VPN Gateway.
  - ii) Perform a variety of administrator actions on the VPN Gateway.
  - iii) Verify a log entry was created for each action taken in Step ii that required the identity of the user, super user privileges and also states the escalation or privileges.
  - iv) Revert back to the baseline configuration, eliminating the changes made in Step ii.
  - v) Repeat above with the Auditor role.
- c) Changes to time. (WLAN-AU-22, WLAN-AU-9)
  - i) Log into the Administration Workstation as an administrator to the VPN Gateway.
  - ii) Modify the system time on the VPN Gateway by at least 1 hour.
  - iii) Verify a log entry was created to indicate the change in system time and by whom.
  - iv) Set the system time back to the accurate time of day.
- d) Log into and out of the Campus WLAN Solution as a normal user and send traffic to the Red network. Then log into the administration log server as an Auditor, and inspect the audit entry for the following:
  - i) Identifies the subject accessing the solution. (WLAN-AU-12)
  - ii) Identify the type of event. (WLAN-AU-10)
  - iii) Identify the success of a normal user sending traffic. (WLAN-AU-11)
  - iv) State the time, date, and time zone offset. (WLAN-AU-8)
  - v) Identify the source address of the event. (WLAN-AU-13)
- e) Establish and terminate a VPN Gateway tunnel. Verify in the logs, that these two events were logged. (WLAN-AU-18, WLAN-AU-19)
- f) Associate and disassociate between the Wireless System and WLAN Client. Verify in the logs, that these two events were logged. (WLAN-AU-20, WLAN-AU-21)
- g) All built-in self test results, which may indicate failures in cryptographic functionality. (WLAN-AU-17)
  - i) Completely power down the VPN Gateway.
  - ii) Power up the VPN Gateway to allow automatic self test.

- iii) Verify a log entry was created during self-test.
- h) Log into the VPN Gateway as an Auditor and offload the previous week's audit log. Verify that the log recorded this action. (WLAN-AU-1)
- i) Log into the VPN Gateway as an Auditor and attempt to change a configuration. Verify that the log recorded this action. (WLAN-AU-3)
- 2) As a normal user, log into the EUD with an incorrect password. As an auditor verify in the logs that this event was detected. (WLAN-AU-25)
- 3) As a normal user, log into the EUD and then log out of the device. As an auditor verify in the log that this event was detected. (WLAN-AU-26)
- 4) As an administrator install software on the EUD. As an Auditor verify in the logs that this event was detect. (WLAN-AU-27)
- 5) As a normal user attempt to disable the WLAN Client. As an Auditor verify in the logs that this event took place. (WLAN-AU-28)
- 6) Inspect the organization's implementing policy states audit logs are monitored by the Auditor at least weekly. (WLAN-AU-16)
- 7) Simultaneous connections.
  - a) Send traffic from a EUD and a EUD that is masquerading as a legitimate device. As a Security Administrator view the traffic and immediately drop the sessions. (WLAN-AU-15)
  - b) Verify that the Certificate Authority Administrator has revoked the device certificate and updated the Certification Revocation List to the Security Administrator. (WLAN-AU-14)
- 8) Verify there is a procedure detailed in the CPS documentation for auditing each CA device within the solution. (WLAN-AU-7)
- 9) Log into the WIDS and verify that event monitoring can only be done through SSHv2, IPsec, or TLS. (WLAN-AU-23)
- 10) As a normal user log into the EUD and send unauthorized traffic to the Red network. As an auditor log into the VPN Gateway. Verify that packets that are blocked are logged. (WLAN-AU-6)
- 11) Access a sensor and turn off the power to the device. Verify that the WIDS logs the communication failure. (WLAN-AU-24)
- 12) As a normal user, unlock the EUDandverify that the action is recorded in the logs. (WLAN-AU-31)
- 13) As a normal user, log into the EUD and turn on Bluetooth setting. As an auditor, verify that the action was logged. (WLAN-AU-32)

For all of these steps, all occurrences of an auditable event shall produce a logged entry.

# 13.29 Configuration Change Detection

This section contains a procedure for ensuring that changes made to any of the Campus WLAN components configurations are detected by the Configuration Change Detection tool.

Requirements being tested: WLAN-CM-1 through WLAN-CM-5

#### **Procedure Description:**

- 1) The following steps shall be performed for each of the Campus WLAN components within the solution.
  - a) Log into the Campus WLAN component.
  - b) Compare the current version of the Campus WLAN components configuration with the stored baseline and ensure the current version matches the stored configuration. (WLAN-CM-1)
  - c) Make a change to the configuration, preferably something that is not fundamental to the security of the Campus WLAN solution. (WLAN-CM-3)
  - d) Look in the audit log to determine if a log entry has been generated about the configuration change and that the changes from c) are recorded. (WLAN-CM-2, WLAN-CM-4)
  - e) Obtain the configuration file and verify that FIPS mode is enabled. (WLAN-CM-5)

#### **Expected Results:**

The Auditor will validate the baseline configuration was stored in Step 1b In Step 1d, there should be a log entry created for the configuration change in the audit log including the actual configuration change. In step 1e, FIPS mode should be enabled for all components.

## 13.30 CA Configurations

This section contains a procedure to ensure that the configurations for all of the CAs used within the Campus WLAN solution follow the requirements given in this package.

**Requirements being tested:** WLAN-KM-1 through WLAN-KM-24, WLAN-KM-26 through WLAN-KM-30 **Procedure Description:** 

- 1) Verify requirements WLAN-KM-1 through WLAN-KM-7, WLAN-KM-10, WLAN-KM-11, and WLAN-KM-14, WLAN-KM-19 through WLAN-KM-24 are met by both CAs.
- 2) Ensure there is certificate revocation information on VPN Gateway, WLAN Clients, and WLAN Authentication Server. (WLAN-KM-8)
- 3) Review the implementing organization's policy for how new certificates are to be issued. As a Certificate Authority Administrator issue a certificate for a new user in accordance with the policy. (WLAN-KM-9)
- 4) Verify requirements WLAN-KM-12, WLAN-KM-13, WLAN-KM-15, WLAN-KM-18, WLAN-KM-29, WLAN-KM-30 are met by locally-run CAs.
- 5) Verify if the Inner tunnel CA and Outer tunnel CA are an Enterprise CA that it meets requirements WLAN-KM-16 and WLAN-KM-17.
- 6) Inspect the WLAN CA to ensure that the CA is connected to the Gray Management network. (WLAN-KM-32)
- 7) Obtain the WLAN CA's configuration file.

- a) Verify that the certificate issue to the WLAN Authentication Server contains the required specification. (WLAN-KM-26)
- b) Verify that the certificate issue to the Wireless System contains the required specification. (WLAN-KM-27)
- c) Verify that the certificate issue to the WLAN Client contains the required client authentication OID. (WLAN-KM-28)

For steps 1-7, all CAs should be configured to meet the requirements of this Capability Package.

# 13.31 Use of Revoked Certificates

This section contains a procedure to ensure that only valid certificates are accepted. This section focuses on certificates that have been revoked (and are therefore invalid) and does not include all types of validity testing.

Requirements being tested: WLAN-KM-33, WLAN-KM-34, WLAN-AU-30

## **Procedure Description:**

- 1) Ensure the solution is in its default setting and that the WLAN Client and VPN connections are established with the proper, valid certificates are used to authenticate the tunnels.
- 2) Revoke a certificate for the VPN Gateway and WLAN Client (or install an alternate revoked certificate on the VPN Gateway and WLAN Client), and ensure the solution is configured so that this revoked certificate will be used for authentication.
  - a) Start the connection.
  - b) Verify that the connection is not successful; end-to-end communication is not provided because the Gateway and the WLAN Controller will fail to authenticate the revoked certificate. Verify the failures are logged in audit data on the EUD. (WLAN-KM-33 WLAN-KM-34, WLAN-AU-30)
- 3) When this testing is complete, remove the revoked certificates and return the configuration to its proper settings. Verify that an entry to the Audit log has been created due to certificate deletion.

#### **Expected Results:**

Authentication will not occur when the VPN Gateway and WLAN Controller cannot verify the validity of the certificates, provided the solution is configured correctly. All results are expected to be pass/fail.

## 13.32 Use of Certificates from Trusted CAs

This section contains a procedure to ensure that public/private key and certificates are only used for authentication only from trusted CAs are accepted.

Requirements being tested: WLAN-KM-35

## **Procedure Description:**

1) Ensure the solution is in its default setting and that the WLAN Client and VPN connections are established with the proper, valid certificates are used to authenticate the tunnels.

- 2) Install approved certificates on the VPN Gateway and WLAN Controller generated by the approved CAs and configure the solution so that the VPN Gateway and WLAN Controller uses these certificates for authentication. (WLAN-KM-35)
  - a) Verify an audit log has been created due to certificate loading.
  - b) Start the connections using the new configuration.
  - c) Verify the connection is successful; end-to-end communication is provided because of the successful authentication. Verify that success is logged in the audit data.
- 3) When this testing is complete, remove the revoked certificates and return the configuration to its proper settings. Verify that an entry to the Audit log has been created due to certificate deletion.

Authentication will occur when the VPN Gateway and WLAN Controller identify the trust anchor of the certificates, provided the solution is configured correctly. All results are expected to be pass/fail.

# 13.33 Implementation of NIDS

This section contains a procedure to ensure that network intrusion detection system (NIDS) is monitoring network activity.

Requirements being tested: WLAN-NI-1 through WLAN-NI-3

#### **Procedure Description:**

- 1) Log into the NIDS on the Gray Management network and verify traffic leaving or arriving to the Wireless System. (WLAN-NI-1)
- 2) Log into the NIDS and verify that all inbound and outbound traffic that matches the attack signatures is reported. (WLAN-NI-2)
- 3) Review the implementing organization's policy to ensure the NIDS's attack signature is updated regularly. (WLAN-NI-3)

**Expected Results:** 

For steps 1-3, the NIDS will be configured correctly according to the requirements of the CP.

# 13.34 Implementation of VPN Gateway

This section contains a procedure to ensure that the VPN Gateway follow the requirements given in this Capability Package.

Requirements being tested: WLAN-VG-1 through WLAN-VG-6, WLAN-KM-25

- 1) For the VPN Gateway in the solution perform the following:
  - a) Access the current configuration for the VPN component.
  - b) Verify a unique device certificate is loaded with the corresponding CA signing certificate. (WLAN-VG-1)

- c) Ensure the corresponding CA signing certificate and certificate revocation information is on the VPN Component. (WLAN-VG-4)
- d) Verify that split tunneling is not enabled. (WLAN-VG-3)
- 2) On the VPN Gateway, perform the following: (WLAN-VG-2)
  - a) Identify the location of the private key store.
  - b) From each interface attempt to access and view the private keys.
  - c) Verify that only from a management interface and with proper credentials the private keys were accessible.
- 3) For VPN authentication check, perform the following: (WLAN-VG-5, WLAN-VG-6, WLAN-KM-25)
  - a) As a Security Administrator, review the VPN Gateway authentication settings. Verify that the certificate based authentication is enabled.
  - b) Identify the database containing the list of clients approved to connect to the VPN Gateway.
  - c) Review the database to verify that field being validated is the Distinguished Name or Subject Alternative Name.
  - d) Review the VPN settings to verify the settings for validating a client matches the database setting.
  - e) Attempt to connect to a client and VPN Gateway that does not appear in the database.
  - f) Verify that the connection failed.

For steps 1-3, the VPN Gateway will be configured according to this Capability Package.

# 13.35 VPN Component Configuration

This section contains a procedure to ensure the VPN Components (VPN Gateway and VPN Client) follow the requirements given in this Capability Package.

Requirements being tested: WLAN-CR-1 through WLAN-CR-19

#### **Procedure Description:**

- 1) Obtain the configuration file for the VPN Components and verify that requirements WLAN-CR-1 through WLAN-CR-5, WLAN-CR-14 through WLAN-CR-19 are met.
- 2) Review the cryptographic settings for the VPN Components and verify that requirements WLAN-CR-6 through WLAN-CR-11 are met.
- 3) Obtain the VPN Gateway IPsec configuration settings and verify that the IPsec SA lifetime is set to 8 hours or less. (WLAN-CR-12)
- 4) Obtain the VPN Gateway IKE configuration settings and verify that IKE SA lifetime is set to 24 hours. (WLAN-CR-13)

#### **Expected Results:**

For steps 1-5, the VPN Components will be configured according to this Capability Package.

# 13.36 Implementation of Port Filtering

This section contains a procedure to ensure the port filtering is implemented on the VPN Gateway, Wireless System, and EUD.

Requirements being tested: WLAN-PF-1 through WLAN-PF-9

#### **Procedure Description:**

- 1) Obtain the firewall settings Wireless System and EUD and verify that only WPA2 is the only authorized for inbound and outbound traffic. (WLAN-PF-1)
- 2) Obtain the firewall settings for Wireless System and VPN Gateway and verify EAP-TLS, IPsec, and control plane protocols are the only authorized for inbound and outbound traffic. (WLAN-PF-2)
- 3) Verify that the configuration files state that communications from the EUD to a third party to be blocked. (WLAN-PF-5)
- 4) Verify that the configuration files state that communications from the EUD to a third party to be disabled. (WLAN-PF-6)
- 5) From the list of authorized EUD addresses, verify that the VPN Gateway firewall settings is limited to the specified range. (WLAN-PF-3)
- 6) From the list of authorized VPN Gateway addresses, verify that the EUD firewall setting is limited to the specified range. (WLAN-PF-4)
- 7) From the Administration Workstation on the Gray Management network, review the Wireless System configuration setting and verify that only the IP address and ports required for management of the device is present. (WLAN-PF-7)
- 8) From the Administration Workstation on the Gray Management network, review the Wireless System configuration. Verify that the WLAN MAC address located in the configuration adheres to authorized EUD MAC address list. (WLAN-PF-8)
- 9) Verify that the firewall configuration for the EUD's Gray network interface is configured to only permit traffic originating from the VPN Gateway and Administration Workstations on the Gray network. (WLAN-PF-9)

#### **Expected Results:**

Port filtering on these components is configured according to the requirements in this Capability Package.

# 13.37 Implementation of WIDS

This section contains a procedure to ensure the Wireless Intrusion Detection System (WIDS) is implemented correctly.

Requirements being tested: WLAN-WI-1 through WLAN-WI-52

#### **Procedure Description:**

1) Obtain a list of authorized wireless network devices. Log into the configuration file and verify that those wireless network devices are on the whitelist. (WLAN-WI-1)

- 2) As a security administrator, verify the WIDS security policy adheres to WLAN-WI-2 through WLAN-WI-9, WLAN-WI-11, WLAN-WI-17, WLAN-WI-19, and WLAN-WI-21-WLAN-WI-22.
- 3) Review WIDS configuration file to verify WLAN-WI-32 through WLAN-WI-36 are met.
- 4) Using an unauthorized EUDs and an authorized access points connect to the Campus WLAN network, perform the following:
  - a) Send traffic from the unauthorized EUD to the access point.
  - b) Apply a sniffer on the WIDS to examine traffic.
  - c) Verify that WIDS detect the frames. (WLAN-WI-10)
- 5) Log into the WIDS configuration file and verify that wireless transmission is not enabled. (WLAN-WI-12)
- 6) Review the WIDS configuration file and verify that Suite B encryption is implemented. (WLAN-WI-13)
- 7) Review the WIDS configuration file and verify two-way authentication is enabled. (WLAN-WI-14)
- 8) Using an authorized EUD and an authorized access point. Perform the following:
  - a) Send traffic from the EUD to the Red Network.
  - b) Apply a sniffer to the WIDS.
  - c) Review traffic to ensure that WIDS comply with WLAN-WI-15.
- 9) Review the WIDS configuration settings for radio interface to ensure that all 802.11 channels GHz bands specified in WLAN-WI-16.
- 10) Review the WIDS configuration to verify that geo-location is enabled for IEEE 802.11 wireless hardware. (WLAN-WI-18)
- 11) Verify that the WIDS is configured to detect and log the following requirements: WLAN-WI-20, WLAN-WI-23 through WLAN-WI-27, WLAN-WI-30, WLAN-WI-39 through WLAN-WI-40, WLAN-WI-42 through WLAN-WI-45, and WLAN-WI-47 through WLAN-WI-50.
- 12) Observe a period of seven days of network traffic. After observing this information perform the following: (WLAN-WI-31, WLAN-WI-37)
  - a) Connect EUD to the network as a normal user.
  - b) Send an abnormal amount of traffic to the Red network.
  - c) As a Security Administrator, observe if the WIDS generates an alarm on this activity.
- 13) Review the WIDS configuration file and to ensure the device computes a network traffic baseline. (WLAN-WI-28)
- 14) As a Security Administrator log into the WIDS configuration console and establish a new network traffic baseline. (WLAN-WI-29)
- 15) Using an unauthorized EUD. Perform the following:
  - a) Attempt to connect to the Campus WLAN network.
  - b) Access the WIDS to verify the unauthorized device has been detected. (WLAN-WI-41)

- 16) Access the WIDS configuration to verify non-secure communication paths for system updates and event monitoring are disabled. (WLAN-WI-51)
- 17) Turn off the Wireless System. Verify that the WIDS issues an alert about the communication failure. (WLAN-WI-52)

#### **Expected Results:**

WIDS on these components is configured according to the requirements in this Capability Package.

# 13.38 CA Configurations

This section contains a procedure to ensure that the configurations for all of the CAs used within the Campus WLAN solution follow the requirements given in this package.

**Requirements being tested:** WLAN-KM-1 through WLAN-KM-24, WLAN-KM-26 through WLAN-KM-30 **Procedure Description:** 

- 1) Verify requirements WLAN-KM-1 through WLAN-KM-7, WLAN-KM-10, WLAN-KM-11, and WLAN-KM-14, WLAN-KM-19 through WLAN-KM-24 are met by both CAs.
- 2) Ensure there is certificate revocation information on VPN Gateway, WLAN Clients, and WLAN Authentication Server. (WLAN-KM-8)
- 3) Review the implementing organization's policy for how new certificates are to be issued. As a Certificate Authority Administrator issue a certificate for a new user in accordance with the policy. (WLAN-KM-9)
- 4) Verify requirements WLAN-KM-12, WLAN-KM-13, WLAN-KM-15, WLAN-KM-18, WLAN-KM-29, WLAN-KM-30 are met by locally-run CAs.
- 5) Verify if the Inner tunnel CA and Outer tunnel CA are an Enterprise CA that it meets requirements WLAN-KM-16 and WLAN-KM-17.
- 6) Inspect the WLAN CA to ensure that the CA is connected to the Gray Management network. (WLAN-KM-32)
- 7) Obtain the WLAN CA's configuration file.
  - a) Verify that the certificate issue to the WLAN Authentication Server contains the required specification. (WLAN-KM-26)
  - b) Verify that the certificate issue to the Wireless System contains the required specification. (WLAN-KM-27)
  - c) Verify that the certificate issue to the WLAN Client contains the required client authentication OID. (WLAN-KM-28)

#### **Expected Results:**

For steps 1-7, all CAs should be configured to meet the requirements of this Capability Package.

# APPENDIX A. HIGH LEVEL DESCRIPTION OF A END USER DEVICE INFRASTRUCTURE CONNECTION

The following summarizes the sequence of events that occur in order to establish network access from a wireless End User Device in the architecture:

- 1. The End User Device is powered on. The WLAN Client automatically associates with the Wireless System.
- 2. The Wireless System requires the WLAN Client to perform an IEEE 802.1X authentication before providing access. The WLAN Client and WLAN Authentication Server mutually authenticate using ITU-T X.50v39 device certificates. The Wireless System acts as a pass through to WLAN Authentication Server during these communications. If either WLAN Authentication Server or the WLAN Client determines that the other party's certificate is not valid, communication will cease.
- 3. The WLAN Client and WLAN Authentication Server execute a key establishment protocol (EAPTLS) to derive the PMK.

- 4. WLAN Authentication Server passes the PMK to the Wireless System using RADIUS inside an IPsec protected wired connection. Depending on the vendor, the Wireless System will either keep the PMK on the Wireless Controller or securely push the keys out to the appropriate AP as needed.
- 5. The WLAN Client and Wireless System perform a 4-way handshake to derive a session key from the PMK. From this point forward all communication between the Wireless Client and the Wireless System is protected with this session key.
- 6. The VPN Client and VPN Gateway mutually authenticate via ITU-T X.509v3 device certificates. If either the VPN Client or the VPN Gateway determines that the other party's certificate is not valid, all communications will cease.
- 7. The VPN Client and VPN Gateway negotiate keys, algorithms, and parameters for the IPsec connection using IKE. From this point forward all communication between the VPN Client and VPN Gateway is protected with an IPsec tunnel.
- 8. At this point the End User Device is connected to the wired network, but does not have access to services. Unless the system owner wants to establish a user authentication method specifically for wireless users, the End User Device and the network perform a user authentication to gain service access using the authentication method already implemented on the wired network.

#### APPENDIX B. GLOSSARY OF TERMS

**Accreditation**—The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. (NIST SP 800-37)

**Authorizing Official (AO)**—A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. (NIST SP 800-53)

**Assurance**—A measure of confidence that the security features and architecture of an Automated Information System (AIS) accurately mediate and enforce the security policy. The certification by designated technical personnel of the extent to which design and implementation of the system meets specified technical requirement for achieving adequate data security.

**Auditing**—The activity of monitoring the operation of a product from within the product. It includes monitoring of a product for a set of pre-determined events. Each audit event may indicate rogue behavior, or a condition that is detrimental to security, or provide necessary forensics to identify the source of rogue behavior.

**Audit log**—A chronological record of the audit events that have been deemed critical to security. The audit log can be used to identify potentially malicious activity that may further identity the source of an attack, as well as potential vulnerabilities where additional countermeasures or corrective action are required.

**Availability**—Assurance that the system and its associated assets are accessible and protected against denial or service attacks, as well as available when the user needs them and in the form needed by the user.

**Black box testing**—Testing the functionality of a component of the solution, such that testing is limited to the subset of functionality that is available from the external interfaces of the box during its normal operational configuration without any additional privileges (such as given to the Security Administrator or Auditor).

**Capability Package**—The set of guidance provided by NSA that describes recommended approaches to composing COTS devices to protect classified information for a particular class of security problem. This package will point to potential products that can be utilized as part of this solution.

**Certification**—The technical evaluation of a system's security features, made as part of and in support of the approval/accreditation process that establishes the extent to which a particular computer system design and implementation meets a set of specified security requirements.

Certification and Accreditation (C&A)—A comprehensive assessment of the management operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. In conjunction with the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. (NIST SP 800-37)

**Certificate Authority (CA)**—An authority trusted by one or more users to create and assign certificates. [ISO 9594-8]

**Certificate Policy (CP)**—A named set of rules that indicate the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular CP might indicate applicability of a type of certificate to the authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range. [RFC 3647]

**Committee on National Security Systems Policy No. 15 (CNSSP-15)**—Policy specifies which public standards may be used for cryptographic protocol and algorithm interoperability to protect National Security Systems (NSS).

**Confidentiality**—Assurance that the data stored in, processed by, or transmitted by the system are protected against unauthorized disclosure and confidence in that only the appropriate set of individuals or organizations would be provided the information.

**Edge Device**—Another term for End User Device as described in this Capability Package, frequently used in Key Management requirements.

**External Interface**—The interface on a VPN device that connects to the outer network (i.e., the Mobility Gray network on the VPN device or the Wireless network on the WLAN device).

**Federal Information Processing Standard (FIPS)**—A set of standards that describes the handling and processing of information within governmental agencies.

**Gray Box testing**—The ability to test functionality within a component of the solution, such that full management privileges are granted (i.e., knowing passwords for security administrator and Auditor and access to the capabilities associated with those privileges). In addition, the use of any and all testing equipment and/or testing software used inside and outside the developed solution is available.

**Protection Profile**—A document used as part of the certification process according to the Common Criteria. As the generic form of a security target, it is typically created by a user or user community and provides an implementation independent specification of information assurance security requirements.

**Public Key Infrastructure (PKI)**—Framework established to issue, maintain, and revoke public key certificates.

**Supply Chain Risk Management (SCRM)** )—A program to establish processes and procedures to minimize acquisition-related risks to critical acquisitions including, hardware components and software solutions from supply chain threats due to reliance on global sources of supply.

**Wireless Intrusion Detection System (WIDS)**—A group of sensors and a central controller working together to provide 24/7 monitoring of the IEEE 802.11 wireless spectrum for intrusion attempts, denial of service attacks, unauthorized devices attempting to connect, and authorized devices that are not following the defined security profile.

# APPENDIX C. ACRONYMS LIST

| Acronym | Definition   |
|---------|--|
| A/C     | Architecture/Configuration                                     |
| AAA     | Authentication, Authorization, and Accounting                  |
| ACL     | Access Control List  |
| AES     | Advanced Encryption Standard                                   |
| AIS     | Automated Information System                                   |
| AO      | Authorizing Official/Approving Official                        |
| AP      | Access Point   |
| API     | Application Program Interface                                  |
| APT     | Advanced Persistent Threat                                     |
| ASCII   | American Standard Code for Information Interchange             |
| AU      | Requirements for Auditing                                      |
| C&A     | Certification and Accreditation                                |
| CA      | Certificate Authority  |
| CAA     | Certificate Authority Administrator                            |
| CBC     | Cipher Block Chaining  |
| CCD     | Configuration Change Detection                                 |
| CCM     | Counter with Cipher Block Chaining Message Authentication Code |
| CM      | Cryptographic Module   |
| CNSS    | Committee on National Security Systems                         |
| CNSSD   | Committee on National Security Systems Directive               |
| CNSSI   | Committee on National Security Systems Instruction             |
| CNSSP   | Committee on National Security Systems Policy                  |
| COTS    | Commercial Off-The-Shelf                                       |
| СР      | Certificate Policy   |
| CPS     | Certification Practice Statement                               |
| CRC     | Cyclic Redundancy Check  |
| CRL     | Certificate Revocation List                                    |
| CSfC    | Commercial Solutions for Classified                            |

| Acronym | Definition  |
|---------|---|
| DA      | Device Administration                                     |
| DAR     | Data-At-Rest  |
| dB      | Decibel   |
| DH      | Diffie-Hellman  |
| DISA    | Defense Information Systems Agency                        |
| DN      | Distinguished Name  |
| DoD     | Department of Defense                                     |
| DoDI    | DoD Instruction   |
| DoS     | Denial-of-Service   |
| DPI     | Deep Packet Inspection                                    |
| DSS     | Digital Signature Standard                                |
| EAP     | Extensible Authentication Protocol                        |
| ECC     | Elliptic Curve Cryptography                               |
| ECDH    | Elliptic Curve Diffie-Hellman                             |
| ECDHE   | Elliptic Curve Diffie-Hellman Ephemeral                   |
| ECDSA   | Elliptic Curve Digital Signature Algorithm                |
| ECP     | Elliptic Curve modulo a Prime                             |
| ESP     | Encapsulating Security Payload                            |
| EUD     | End User Device   |
| FDE     | Full Disk Encryption                                      |
| FIPS    | Federal Information Processing Standard                   |
| FTP     | File Transfer Protocol                                    |
| FW      | Firewall  |
| GHz     | Gigahertz   |
| GOTS    | Government Off-The-Shelf                                  |
| GTK     | Group Temporal Key  |
| GUI     | Graphical User Interface                                  |
| HIDS    | Host-based Intrusion Detection System                     |
| HMAC    | Hash-based Message Authentication Code                    |
| HTTP    | Hyper Text Transfer Protocol                              |
| HTTPS   | Hyper Text Transport Protocol Secure                      |
| IA      | Information Assurance                                     |
| IAD     | Information Assurance Directorate                         |
| IAVA    | Information Assurance Vulnerability Alert                 |
| IDS     | Intrusion Detection System                                |
| IEEE    | Institute of Electrical and Electronic Engineers          |
| IETF    | Internet Engineering Task Force                           |
| IKE     | Internet Key Exchange                                     |
| IKEv2   | Internet Key Exchange Version 2                           |
| IP      | Internet Protocol   |
| IPS     | Intrusion Prevention System                               |
| IPsec   | Internet Protocol Security                                |
| ISAKMP  | Internet Security Association and Key Management Protocol |

| Acronym | Definition   |
|---------|--|
| ISO     | International Organization for Standardization                                   |
| ITU     | International Telecommunication Union  |
| ITU-T   | International Telecommunication Union – Telecommunication Standardization Sector |
| KM      | Key Management   |
| LAN     | Local Area Network   |
| MAC     | Medium Access Control  |
| MDM     | Mobile Device Management   |
| NAC     | Network Access Controller  |
| NDPP    | Network Device Protection Profile  |
| NIAP    | National Information Assurance Partnership                                       |
| NIDS    | Network-based Intrusion Detection System   |
| NIST    | National Institute of Standards and Technology                                   |
| NPE     | Non-Person Entity  |
| NSA     | National Security Agency   |
| NSS     | National Security System   |
| OCSP    | Online Certificate Status Protocol   |
| OID     | Object Identifier  |
| OS      | Operating System   |
| OTA     | Over-The-Air   |
| PF      | Port Filtering   |
| PHY     | Physical Layer   |
| PKCS    | Public Key Cryptography Standard   |
| PKI     | Public Key Infrastructure  |
| PMK     | Pair-wise Master Key   |
| PP      | Protection Profile   |
| PSK     | Pre-Shared Key   |
| RADIUS  | Remote Authentication Dial In User Service                                       |
| RAS     | Remote Access Server   |
| RF      | Radio Frequency  |
| RFC     | Request for Comments   |
| RI      | Remote Interface   |
| RSA     | Rivest, Shamir, Adelman  |
| S       | SECRET   |
| S3      | Secure Sharing Suite   |
| SA      | Security Association   |
| SCRM    | Supply Chain Risk Management   |
| SFTP    | Secure File Transfer Protocol  |
| SHA     | Secure Hash Algorithm  |
| SHS     | Secure Hash Standard   |
| SIPRNet | SECRET Internet Protocol Router Network  |
| SNMP    | Simple Network Management Protocol   |
| SP      | (NIST) Special Publication   |
| SRC     | Secure Remote Computing  |

| Acronym | Definition                              |
|---------|---|
| SSH     | Secure Shell                            |
| SSID    | Service Set Identifier                  |
| STIG    | Security Technical Implementation Guide |
| TLS     | Transport Layer Security                |
| TS      | TOP SECRET                              |
| UDP     | User Datagram Protocol                  |
| USG     | United States Government                |
| VC      | VPN Client                              |
| VG      | VPN Gateway                             |
| VLAN    | Virtual Local Area Network              |
| VM      | Virtual Machine                         |
| VPN     | Virtual Private Network                 |
| WC      | WLAN Client                             |
| WIDS    | Wireless Intrusion Detection System     |
| Wi-Fi   | Wireless Fidelity                       |
| WLAN    | Wireless Local Area Network             |
| WPA     | Wi-Fi Protected Access                  |
| WPA2    | Wi-Fi Protected Access 2                |
| WS      | WLAN System                             |

# APPENDIX D. REFERENCES

The standards listed in this table may be periodically updated or superseded by their respective standards organizations. Each version of this Capability Package references the relevant standards at time of publication. If a vendor claims compliance to a more recent version of a standard than the one listed, contact NSA for guidance.

| CNSSI 4009                               | CNSS Instruction (CNSSI) 4009, National Information Assurance (IA) Glossary Committee for National Security Systems http://www.cnss.gov/Assets/pdf/cnssi 4009.pdf   | April 2010    |
|--|---|---------------|
| CNSSD 505                                | CNSS Directive (CNSSD) 505, Supply Chain Risk Management  | March 2012    |
| CNSSI 1300                               | CNSSI 1300, Instruction For National Security Systems Public<br>Key Infrastructure X.509 Certificate Policy   | June 2011     |
| CNSSP 15                                 | CNSS Policy (CNSSP) Number 15, National Information<br>Assurance Policy on the Use of Public Standards for the Secure<br>Sharing of Information Among National Security Systems,<br>Committee on National Security Systems  | October 2012  |
| DoDI 8420.01                             | DoD Instruction 8420.01, Commercial Wireless Local-Area<br>Network (WLAN) Devices, Systems, and Technologies  | November 2009 |
| FIPS 140-2                               | Federal Information Processing Standard (FIPS) 140-2, Security Requirements For Cryptographic Modules. http://csrc.nist.gov/publications/fips/fips 140-2/fips1402.pdf   | May 2001      |
| FIPS 180-4                               | Federal Information Processing Standard (FIPS) 180-4, Secure Hash Standard (SHS). http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf   | March 2012    |
| FIPS 186-3                               | Federal Information Processing Standard (FIPS) 186-3, Digital Signature Standard (DSS). http://csrc.nist.gov/publications/fips/fips186-3/fips 186-3.pdf   | June 2009     |
| FIPS 197                                 | Federal Information Processing Standard (FIPS) 197, Advanced Encryption Standard (AES). http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf   | November 2001 |
| IEEE 802.1X                              | IEEE 802.1X, Port-based Network Access Control  | February 2010 |
| IEEE 802.11                              | IEEE 802.11-2012, Standard for Information technology-<br>Telecommunications and information exchange between<br>systems Local and metropolitan area networks—Specific<br>requirements Part 11: Wireless LAN Medium Access Control<br>(MAC) and Physical Layer (PHY) Specifications | March 2012    |
| ITU-T X.509                              | International Telecommunication Union (ITU) Recommendation X.509, Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks  | November 2008 |
| NIAP<br>Authentication<br>Server PP      | Authentication Server Protection Profile. <a href="http://www.niap-ccevs.org/pp/draft_pps/">http://www.niap-ccevs.org/pp/draft_pps/</a>   | TBD           |
| NIAP IPsec VPN<br>Client PP              | IPsec VPN Client Protection Profile. http://www.niap-<br>ccevs.org/pp   | January 2012  |
| NIAP IPsec VPN<br>Gateway EP             | IPsec VPN Gateway Extended Package. http://www.niap-<br>ccevs.org/pp/draft_pps/   | April 2013    |
| NIAP Stateful<br>Traffic Filter FW<br>EP | Network Device Protection Profile (NDPP) Extended Package<br>Stateful Traffic Filter Firewall   | December 2011 |

| NIAP WLAN<br>Access System PP  | Protection Profile for Wireless Local Area Network (WLAN) Access System. http://www.niap-ccevs.org/pp/draft_pps/   | November 2011 |
|--------------------------------|--|---------------|
| NIAP WLAN<br>Client PP         | Protection Profile for Wireless Local Area Network (WLAN) Client. http://www.niap-ccevs.org/pp/draft_pps/  | November 2011 |
| NIAP Mobile<br>Endpoint OS PP  | Mobile Endpoint Operating System Protection Profile.<br>http://www.niap-ccevs.org/pp/draft_pps/  | January 2013  |
| NIAP Mobile<br>Endpoint App PP | Mobile Endpoint Application Protection Profile.<br>http://www.niap-ccevs.org/pp/draft_pps/   | TBD           |
| NIST SP 800-37                 | National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems, Revision 1. http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf   | February 2010 |
| NIST SP 800-38A                | National Institute of Standards and Technology (NIST) Special Publication (SP) 800-38A, Recommendation for Block Cipher Modes of Operation. M. Dworkin. <a href="http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf">http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf</a>  | December 2001 |
| NIST SP 800-38C                | National Institute of Standards and Technology (NIST) Special Publication (SP) 800-38C, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality. M. Dworkin. <a href="http://csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C">http://csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C</a> updated-July20 2007.pdf | May 2004      |
| NIST SP 800-38D                | National Institute of Standards and Technology (NIST) Special Publication (SP) 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. M. Dworkin. <a href="http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf">http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf</a>                                | November 2007 |
| NIST SP 800-53                 | NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations, Revision 3.<br>http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf   | August 2009   |
| NIST SP 800-56A                | NIST Special Publication 800-56A. Recommendation for Pair-<br>Wise Key Establishment Schemes Using Discrete Logarithm<br>Cryptography. E. Barker, D. Johnson, and M. Smid.<br>http://csrc.nist.gov/publications/nistpubs/800-56A/SP800-<br>56A Revision1 Mar08-2007.pdf  | March 2007    |
| NIST SP 800-56C                | NIST Special Publication 800-56C, Recommendation for Key Derivation through Extraction-then-Expansion. L. Chen. <a href="http://csrc.nist.gov/publications/nistpubs/800-56C/SP-800-56C.pdf">http://csrc.nist.gov/publications/nistpubs/800-56C/SP-800-56C.pdf</a>  | November 2011 |
| NSA Suite B                    | NSA Guidance on Suite B Cryptography [including the Secure Sharing Suite (S3)]. http://www.nsa.gov/ia/programs/suiteb cryptography/index.shtml   | November 2010 |
| RFC 2246                       | RFC 2246 The TLS Protocol Version 1.0. T. Dierks and C. Allen. <a href="http://www.ietf.org/rfc/rfc2246.txt">http://www.ietf.org/rfc/rfc2246.txt</a>   | January 1999  |
| RFC 2407                       | RFC 2407 The Internet IP Security Domain Interpretation for ISAKMP. D. Piper. http://www.ietf.org/rfc/rfc2407.txt  | November 1998 |
| RFC 2408                       | RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP). D. Maughan, et.al. http://www.ietf.org/rfc/rfc2408.txt  | November 1998 |

| RFC 2409 | RFC 2409 The Internet Key Exchange (IKE). D. Harkins and D. Carrel. <a href="http://www.ietf.org/rfc/rfc2409.txt">http://www.ietf.org/rfc/rfc2409.txt</a>   | November 1998  |
|----------|---|----------------|
| RFC 2865 | RFC 2865 Remote Authentication Dial In User Service (RADIUS).<br>C. Rigney, et.al. <a href="http://www.ietf.org/rfc/rfc2865.txt">http://www.ietf.org/rfc/rfc2865.txt</a>  | June 2000      |
| RFC 3579 | RFC 3579 RADIUS (Remote Authentication Dial In User Service) Support for Extensible Authentication Protocol (EAP). B. Aboba and P. Calhoun. <a href="http://www.ietf.org/rfc/rfc3579.txt">http://www.ietf.org/rfc/rfc3579.txt</a>                     | September 2003 |
| RFC 3647 | RFC 3647 Internet X.509 Public Key infrastructure Certificate Policy and Certification Practices Framework Internet Engineering Task Force. S. Chokhani, et.al. <a href="http://www.ietf.org/rfc/rfc3647.txt">http://www.ietf.org/rfc/rfc3647.txt</a> | November 2003  |
| RFC 4106 | RFC 4106 The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP). J. Viega and D. McGrew. <a href="http://www.ietf.org/rfc/rfc4106.txt">http://www.ietf.org/rfc/rfc4106.txt</a>  | June 2005      |
| RFC 4252 | RFC 4252 The Secure Shell (SSH) Authentication Protocol. T. Ylonen and C. Lonvick. <a href="http://www.ietf.org/rfc/rfc4252.txt">http://www.ietf.org/rfc/rfc4252.txt</a>  | January 2006   |
| RFC 4253 | RFC 4253 The Secure Shell (SSH) Transport Layer Protocol. T. Ylonen and C. Lonvick. http://www.ietf.org/rfc/rfc4253.txt   | January 2006   |
| RFC 4254 | RFC 4254 The Secure Shell (SSH) Connection Protocol. T. Ylonen and C. Lonvick. http://www.ietf.org/rfc/rfc4254.txt  | January 2006   |
| RFC 4301 | RFC 4301 Security Architecture for the Internet Protocol. S. Kent and K. Seo. <a href="http://www.ietf.org/rfc/rfc4301.txt">http://www.ietf.org/rfc/rfc4301.txt</a>   | December 2005  |
| RFC 4303 | RFC 4303 IP Encapsulating Security Payload. S. Kent. http://www.ietf.org/rfc/rfc4603.txt  | December 2005  |
| RFC 4307 | RFC 4307 Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2). J. Schiller. http://www.ietf.org/rfc/rfc4607.txt  | December 2005  |
| RFC 4308 | RFC 4308 Cryptographic Suites for IPsec. P. Hoffman. http://www.ietf.org/rfc/rfc4608.txt  | December 2005  |
| RFC 4492 | RFC 4492 Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS). S. Blake-Wilson, et.al. <a href="http://www.ietf.org/rfc/rfc4492.txt">http://www.ietf.org/rfc/rfc4492.txt</a>  | May 2006       |
| RFC 4868 | RFC 4868 Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec. S. Kelly and S. Frankel. http://www.ietf.org/rfc/rfc4868.txt  | May 2007       |
| RFC 5216 | RFC 5216, The EAP-TLS Authentication Protocol. D. Simon, B. Adoba, and R. Hurst. <a href="http://www.ietf.org/rfc/rfc5216.txt">http://www.ietf.org/rfc/rfc5216.txt</a>  | March 2008     |
| RFC 5246 | RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2. T. Dierks and E. Rescorla. http://www.ietf.org/rfc/rfc5246.txt  | August 2008    |
| RFC 5280 | RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. D. Cooper, et.al. <a href="http://www.ietf.org/rfc/rfc5280.txt">http://www.ietf.org/rfc/rfc5280.txt</a>                                  | May 2008       |
| RFC 5289 | RFC 5289 TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM). E. Rescorla. http://www.ietf.org/rfc/rfc5289.txt  | August 2008    |
| RFC 5903 | RFC 5903 Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2. D. Fu and J. Solinas. http://www.ietf.org/rfc/rfc5903.txt   | June 2010      |
| RFC 5996 | RFC 5996 Internet Key Exchange Protocol Version 2 (IKEv2). C. Kaufman, et.al. <a href="http://www.ietf.org/rfc/rfc5596.txt">http://www.ietf.org/rfc/rfc5596.txt</a>   | September 2010 |

| RFC 6379 Suite B Cryptographic Suites for IPsec. L. Law and J. Solinas. <a href="http://www.ietf.org/rfc/rfc6379.txt">http://www.ietf.org/rfc/rfc6379.txt</a>        | October 2011 |
|--|--------------|
| RFC 6460 Suite B Profile for Transport Layer Security (TLS). M. Salter, et.al. <a href="http://www.ietf.org/rfc/rfc6460.txt">http://www.ietf.org/rfc/rfc6460.txt</a> | January 2012 |

# APPENDIX E. EXAMPLE IAD APPROVAL LETTER FOR CAMPUS WLAN CAPABILITY PACKAGES

UNCLASSIFIED





#### **Commercial Solutions For Classified**

#### Information Assurance Directorate Approval

The National Manager for national security systems (NSS) (Director NSA as delegated to NSA's Information Assurance Director) is authorized under National Security Directive No. 42 (NSD-42) to develop and approve information assurance techniques to secure NSS. In executing this authority, the National Manager may provide guidance regarding the appropriate combinations of Commercial Off-the-Shelf IA and IA-enabled Information Technology Products. (See Committee on National Security Systems Policy No. 11, "National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products," dated 10 June 2013".)).

The Campus Wireless Local Area Network (WLAN) Capability Package (CP) Version 1.1 is a technique that has been developed and approved by the National Manager as a commercial strategy suitable for protecting classified information and NSS provided the user's implementation of the solution is configured and maintained as required by the CP.

The user's Authorizing Official (AO) is responsible for ensuring that the user correctly implements the CP. If users need to deviate from the requirements and guidance in the CP before the user's implementation of the solution may be approved and accredited for use, the user must obtain approval for the Capability Package deviation, from their organization's AO and the AO must request and receive NSA approval for this same deviation. A request for a deviation approval must include a detailed justification for the user's deviation from the CP.

The residual risks for this CP are documented in the Campus WLAN CP Version 1.1 Risk Assessment. If an organization implements this solution, the user's AO is responsible for accepting or mitigating the residual risks.

Users of the CP are responsible for obtaining, under their organization's established accreditation and approval processes, certification and accreditation of the user's implementation of the CP.

The registration with NSA of the user's implementation of the CP, along with the applicable AO's assertion that 1) the implementation of the solution is fully compliant with the CP and 2) the residual risk is acceptable or has been sufficiently mitigated, serve as NSA's approval of the user's implementation of this CSfC solution to protect classified and NSS.

| DEBORA A. PLUNKETT    | Date |
|-----------------------|------|
| Information Assurance |      |
| Director              |      |

UNCLASSIFIED

# APPENDIX F. SUMMARY OF CHANGES TO REQUIREMENTS

This appendix summarizes the changes between the requirements in this Capability Package and the requirements in its predecessor, the CSfC Campus WLAN Capability Package version 1.0, dated August 20, 2013. It is provided as an aide to solution owners who have developed a solution compliant with the earlier Capability Package and wish to determine the extent to which their existing solution complies with this Capability Package.

In general, requirements included in the CSfC Campus WLAN Capability Package version 1.0, dated August 30, 2013, are also included in this Capability Package without any substantive changes. The wording used in several requirements has been changed to clarify their intent, and typically a solution that complied with their original wording is expected to also comply with their revised wording.

**Error! Reference source not found.** lists in more detail which requirements from the CSfC Campus WLAN Capability Package version 1.0, dated August 30, 2013, have changed in this Capability Package. Any requirements not listed here have not changed.

# F.1 Changes to Campus WLAN CP version 1.1 Requirements

| WLAN CP 1.0<br>Requirement | Change Description   |
|----------------------------|--|
| WLAN-PS-11                 | Modified to stated differences between Service Packs and version |
|                            | number.  |
| WLAN-WL-2                  | Removed Enterprise and align naming to Red Network data.         |
| WLAN-VC-4                  | Requirement was changed from an objective to threshold meets     |
|                            | objectives.  |
| WLAN-IA-4                  | Changed DH Group to 2 to 14.                                     |
| WLAN-IA-9                  | Requirement removed  |
| WLAN-WI-                   | Requirement removed  |
| WLAN-WI-18                 | Specified IEEE 802.11  |
| WLAN-RA-5                  | Requirement removed  |
| WLAN-TR-1                  | New requirement  |
| WLAN-WI-37                 | Requirement re-worded  |
| WLAN-EU-19                 | Requirement is threshold meets objective                         |
| WLAN-EU-20                 | New requirement  |
| WLAN-CR-9                  | Requirement removed  |
| WLAN-CR-10                 | Requirement removed  |
| WLAN-VC-4                  | Requirement changed from an objective to threshold is objective  |
| WLAN-SR-8                  | Requirement removed  |
| WLAN-GD-2                  | Requirement removed  |
| WLAN-IA-18                 | Requirement removed  |
| WLAN-IA-19                 | New requirement. Added DH Group 19 and/or 20                     |
| WLAN-CR-6-14               | Requirement re-worded  |

| WLAN CP 1.0<br>Requirement | Change Description    |
|----------------------------|-----------------------|
| WLAN-CR-18- 19             | Requirement re-worded |
| WLAN-IA-6                  | Requirement re-worded |
| WLAN-IA-10-11,13           | Requirement re-worded |
| WLAN-KM-19,22              | Requirement re-worded |
| WLAN-PR-5                  | Requirement re-worded |
| WLAN-CR-1,4                | Requirement re-worded |
| WLAN-IA-17                 | Requirement re-worded |